

**H.R. 52, THE FAIR HEALTH INFORMATION  
PRACTICES ACT OF 1997**

---

---

**HEARING**

BEFORE THE  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT  
REFORM AND OVERSIGHT  
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

FIRST SESSION

ON

**H.R. 52**

TO ESTABLISH A CODE OF FAIR INFORMATION PRACTICES FOR  
HEALTH INFORMATION, TO AMEND SECTION 552A OF TITLE 5,  
UNITED STATES CODE, AND FOR OTHER PURPOSES

---

JUNE 5, 1997

---

**Serial No. 105-58**

---

Printed for the use of the Committee on Government Reform and Oversight



U.S. GOVERNMENT PRINTING OFFICE

45-252 CC

WASHINGTON : 1998

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
J. DENNIS HASTERT, Illinois	TOM LANTOS, California
CONSTANCE A. MORELLA, Maryland	ROBERT E. WISE, JR., West Virginia
CHRISTOPHER SHAYS, Connecticut	MAJOR R. OWENS, New York
STEVEN SCHIFF, New Mexico	EDOLPHUS TOWNS, New York
CHRISTOPHER COX, California	PAUL E. KANJORSKI, Pennsylvania
ILEANA ROS-LEHTINEN, Florida	GARY A. CONDIT, California
JOHN M. McHUGH, New York	CAROLYN B. MALONEY, New York
STEPHEN HORN, California	THOMAS M. BARRETT, Wisconsin
JOHN L. MICA, Florida	ELEANOR HOLMES NORTON, Washington, DC
THOMAS M. DAVIS, Virginia	CHAKA FATTAH, Pennsylvania
DAVID M. McINTOSH, Indiana	ELIJAH E. CUMMINGS, Maryland
MARK E. SOUDER, Indiana	DENNIS J. KUCINICH, Ohio
JOE SCARBOROUGH, Florida	ROD R. BLAGOJEVICH, Illinois
JOHN B. SHADEGG, Arizona	DANNY K. DAVIS, Illinois
STEVEN C. LATOURETTE, Ohio	JOHN F. TIERNEY, Massachusetts
MARSHALL "MARK" SANFORD, South Carolina	JIM TURNER, Texas
JOHN E. SUNUNU, New Hampshire	THOMAS H. ALLEN, Maine
PETE SESSIONS, Texas	HAROLD E. FORD, JR., Tennessee
MICHAEL PAPPAS, New Jersey	
VINCE SNOWBARGER, Kansas	BERNARD SANDERS, Vermont
BOB BARR, Georgia	(Independent)
ROB PORTMAN, Ohio	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

JUDITH MCCOY, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

PETE SESSIONS, Texas	CAROLYN B. MALONEY, New York
THOMAS DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
JOE SCARBOROUGH, Florida	MAJOR R. OWENS, New York
MARSHALL "MARK" SANFORD, South Carolina	ROD R. BLAGOJEVICH, Illinois
JOHN E. SUNUNU, New Hampshire	DANNY K. DAVIS, Illinois

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

MARK UNCAPHER, *Counsel*

JOHN HYNES, *Professional Staff Member*

ANDREA MILLER, *Clerk*

DAVID McMILLEN, *Minority Professional Staff Member*

## CONTENTS

---

	Page
Hearing held on June 5, 1997 .....	1
Text of H.R. 52 .....	1
Statement of:	
Condit, Hon. Gary A., a Representative in Congress from the State of California .....	27
Gabriel, Dr. Sherine, Department of Health Services Research, Mayo Clinic, representing the Healthcare Leadership Council; Dr. Elizabeth Andrews, Glaxo Wellcome Inc., representing the Pharmaceutical Research and Manufacturers Association; and Dr. Steven Kenny Hoge, chair, Council on Psychiatry and Law of the American Psychiatric Association .....	97
Goldman, Janlori, visiting scholar, Georgetown University Law Center, and affiliated with the Center for Democracy and Technology; Dr. Donald J. Palmisano, member, Board of Trustees, American Medical Association; and Merida L. Johns, Ph.D., president, American Health Information Management Association .....	53
Stearns, Hon. Cliff, a Representative in Congress from the State of Florida .....	32
Letters, statements, etc., submitted for the record by:	
Andrews, Dr. Elizabeth, Glaxo Wellcome Inc., representing the Pharmaceutical Research and Manufacturers Association:	
Information concerning informed consent .....	158
Prepared statement of .....	116
Condit, Hon. Gary A., a Representative in Congress from the State of California, prepared statement of .....	29
Gabriel, Dr. Sherine, Department of Health Services Research, Mayo Clinic, representing the Healthcare Leadership Council, prepared statement of .....	100
Hoge, Dr. Steven Kenny, chair, Council on Psychiatry and Law of the American Psychiatric Association, prepared statement of .....	128
Johns, Merida L., Ph.D., president, American Health Information Management Association, prepared statement of .....	67
Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York, prepared statement of .....	49
Palmisano, Dr. Donald J., member, Board of Trustees, American Medical Association, prepared statement of .....	59
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of .....	41
Slaughter, Hon. Louise M., a Representative in Congress from the State of New York, prepared statement of .....	43
Stearns, Hon. Cliff, a Representative in Congress from the State of Florida, prepared statement of .....	34



**H.R. 52: THE FAIR HEALTH INFORMATION  
PRACTICES ACT OF 1997**

THURSDAY, JUNE 5, 1997

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION, AND TECHNOLOGY,  
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 9:32 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Sessions, and Maloney.

Staff present: J. Russell George, staff director and chief counsel; Mark Uncapher, counsel; John Hynes, professional staff member; Andrea Miller, clerk; and David McMillen and Ron Stroman, minority professional staff members.

Mr. HORN. The Subcommittee on Government Management, Information, and Technology will come to order.

We are here today to consider the issue of medical records privacy and H.R. 52, the Fair Health Information Practices Act of 1997, introduced by Representative Condit of California.

[The text of H.R. 52 follows:]

105TH CONGRESS  
1ST SESSION

H.R. 52

To establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 7, 1997

MR. CONDIT introduced the following bill; which was referred to the Committee on Commerce, and in addition to the Committees on Government Reform and Oversight, and the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

(1)

**SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) **SHORT TITLE.**—This Act may be cited as the “Fair Health Information Practices Act of 1997”.

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings and purposes.
- Sec. 3. Definitions.

**TITLE I—FAIR HEALTH INFORMATION PRACTICES**

**Subtitle A—Duties of Health Information Trustees**

- Sec. 101. Inspection of protected health information.
- Sec. 102. Amendment of protected health information.
- Sec. 103. Notice of information practices.
- Sec. 104. Disclosure history.
- Sec. 105. Security.

**Subtitle B—Use and Disclosure of Protected Health Information**

- Sec. 111. General limitations on use and disclosure.
- Sec. 112. Authorizations for disclosure of protected health information.
- Sec. 113. Treatment, payment, and oversight.
- Sec. 114. Next of kin and directory information.
- Sec. 115. Public health.
- Sec. 116. Health research.
- Sec. 117. Emergency circumstances.
- Sec. 118. Judicial and administrative purposes.
- Sec. 119. Law enforcement.
- Sec. 120. Subpoenas, warrants, and search warrants.

**Subtitle C—Access Procedures and Challenge Rights**

- Sec. 131. Access procedures for law enforcement subpoenas, warrants, and search warrants.
- Sec. 132. Challenge procedures for law enforcement subpoenas.
- Sec. 133. Access and challenge procedures for other subpoenas.
- Sec. 134. Construction of subtitle; suspension of statute of limitations.
- Sec. 135. Responsibilities of Secretary.

**Subtitle D—Miscellaneous Provisions**

- Sec. 141. Payment card and electronic payment transactions.
- Sec. 142. Access to protected health information outside of the United States.
- Sec. 143. Standards for electronic documents and communications.
- Sec. 144. Duties and authorities of affiliated persons.
- Sec. 145. Agents and attorneys.
- Sec. 146. Minors.
- Sec. 147. Maintenance of certain protected health information.

**Subtitle E—Enforcement**

- Sec. 151. Civil actions.
- Sec. 152. Civil money penalties.
- Sec. 153. Alternative dispute resolution.
- Sec. 154. Amendments to criminal law.

**TITLE II—AMENDMENTS TO TITLE 5, UNITED STATES CODE**

- Sec. 201. Amendments to title 5, United States Code.

**TITLE III—REGULATIONS, RESEARCH, AND EDUCATION; EFFECTIVE DATES; APPLICABILITY; AND RELATIONSHIP TO OTHER LAWS**

- Sec. 301. Regulations; research and education.
- Sec. 302. Effective dates.
- Sec. 303. Applicability.
- Sec. 304. Relationship to other laws.

**SEC. 2. FINDINGS AND PURPOSES.**

(a) **FINDINGS.**—The Congress finds as follows:

(1) The right to privacy is a personal and fundamental right protected by the Constitution of the United States.

(2) The improper use or disclosure of personally identifiable health information about an individual may cause significant harm to the interests of the individual in privacy and health care, and may unfairly affect the ability of the individual to obtain employment, education, insurance, credit, and other necessities.

(3) Current legal protections for health information vary from State to State and are inadequate to meet the need for fair information practices standards.

(4) The movement of individuals and health information across State lines, access to and exchange of health information from automated data banks and networks, and the emergence of multistate health care providers and payors create a compelling need for uniform Federal law, rules, and procedures governing the use, maintenance, and disclosure of health information.

(5) Uniform rules governing the use, maintenance, and disclosure of health information are an essential part of health care reform, are necessary to support the computerization of health information, and can reduce the cost of providing health services by making the necessary transfer of health information more efficient.

(6) An individual needs access to health information about the individual as a matter of fairness, to enable the individual to make informed decisions about health care, and to correct inaccurate or incomplete information.

(b) **PURPOSES.**—The purposes of this Act are as follows:

(1) To define the rights of an individual with respect to health information about the individual that is created or maintained as part of the health treatment and payment process.

(2) To define the rights and responsibilities of a person who creates or maintains individually identifiable health information that originates or is used in the health treatment or payment process.

(3) To establish effective mechanisms to enforce the rights and responsibilities defined in this Act.

**SEC. 3. DEFINITIONS.**

(a) **DEFINITIONS RELATING TO PROTECTED HEALTH INFORMATION.**—For purposes of this Act:

(1) **DISCLOSE.**—The term “disclose”, when used with respect to protected health information that is held by a health information trustee, means to provide access to the information, but only if such access is provided by the trustee to a person other than—

(A) the trustee or an officer or employee of the trustee;

(B) an affiliated person of the trustee; or

(C) a protected individual who is a subject of the information.

(2) **DISCLOSURE.**—The term “disclosure” means the act or an instance of disclosing.

(3) **PROTECTED HEALTH INFORMATION.**—The term “protected health information” means any information, whether oral or recorded in any form or medium—

(A) that is created or received in a State by—

(i) a health care provider;

(ii) a health benefit plan sponsor;

(iii) a health oversight agency; or

(iv) a public health authority;

(B) that relates in any way to the past, present, or future physical or mental health or condition or functional status of a protected individual, the provision of health care to a protected individual, or payment for the provision of health care to a protected individual; and

(C) that—

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(4) **PROTECTED INDIVIDUAL.**—The term “protected individual” means an individual who, with respect to a date—

(A) is living on the date; or

(B) has died within the 2-year period ending on the date.

(5) **USE.**—The term “use”, when used with respect to protected health information that is held by a health information trustee, means—

(A) to use, or provide access to, the information in any manner that does not constitute a disclosure; or

(B) any act or instance of using, or providing access, described in subparagraph (A).

(b) DEFINITIONS RELATING TO HEALTH INFORMATION TRUSTEES.—For purposes of this Act:

(1) CARRIER.—The term “carrier” means a licensed insurance company, a hospital or medical service corporation (including an existing Blue Cross or Blue Shield organization, within the meaning of section 833(c)(2) of the Internal Revenue Code of 1986), a health maintenance organization, or other entity licensed or certified by a State to provide health insurance or health benefits.

(2) HEALTH BENEFIT PLAN.—The term “health benefit plan” means—

(A) any contract of health insurance, including any hospital or medical service policy or certificate, hospital or medical service plan contract, or health maintenance organization group contract, that is provided by a carrier; and

(B) an employee welfare benefit plan or other arrangement insofar as the plan or arrangement provides health benefits and is funded in a manner other than through the purchase of one or more policies or contracts described in subparagraph (A).

(3) HEALTH BENEFIT PLAN SPONSOR.—The term “health benefit plan sponsor” means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a carrier or other person providing a health benefit plan, including any public entity that provides payments for health care items and services under a health benefit plan that are equivalent to payments provided by a private person under such a plan; or

(B) an officer or employee of a person described in subparagraph (A).

(4) HEALTH CARE PROVIDER.—The term “health care provider” means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a person who is licensed, certified, registered, or otherwise authorized by law to provide an item or service that constitutes health care in the ordinary course of business or practice of a profession;

(B) a Federal or State program that directly provides items or services that constitute health care to beneficiaries; or

(C) an officer or employee of a person described in subparagraph (A) or (B).

(5) HEALTH INFORMATION TRUSTEE.—The term “health information trustee” means—

(A) a health care provider;

(B) a health oversight agency;

(C) a health benefit plan sponsor;

(D) a public health authority;

(E) a health researcher; or

(F) a person who, with respect to a specific item of protected health information, is not described in subparagraphs (A) through (E) but receives the information—

(i) pursuant to—

(I) section 117 (relating to emergency circumstances);

(II) section 118 (relating to judicial and administrative purposes);

(III) section 119 (relating to law enforcement); or

(IV) section 120 (relating to subpoenas, warrants, and search warrants); or

(ii) while acting in whole or in part in the capacity of an officer or employee of a person described in clause (i).

(6) HEALTH OVERSIGHT AGENCY.—The term “health oversight agency” means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a person who performs or oversees the performance of an assessment, evaluation, determination, or investigation relating to the licensing, accreditation, or certification of health care providers;

(B) a person who—

- (i) performs or oversees the performance of an audit, assessment, evaluation, determination, or investigation relating to the effectiveness of, compliance with, or applicability of, legal, fiscal, medical, or scientific standards or aspects of performance related to the delivery of, or payment for, health care; and
  - (ii) is a public agency, acting on behalf of a public agency, acting pursuant to a requirement of a public agency, or carrying out activities under a State or Federal statute regulating the assessment, evaluation, determination, or investigation; or
  - (C) an officer or employee of a person described in subparagraph (A) or (B).
- (7) HEALTH RESEARCHER.—The term “health researcher” means a person who, with respect to a specific item of protected health information, receives the information—
- (A) pursuant to section 116 (relating to health research); or
  - (B) while acting in whole or in part in the capacity of an officer or employee of a person described in subparagraph (A).
- (8) PUBLIC HEALTH AUTHORITY.—The term “public health authority” means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—
- (A) an authority of the United States, a State, or a political subdivision of a State that is responsible for public health matters;
  - (B) a person acting under the direction of such an authority; or
  - (C) an officer or employee of a person described in subparagraph (A) or (B).
- (c) OTHER DEFINITIONS.—For purposes of this Act:
- (1) AFFILIATED PERSON.—The term “affiliated person” means a person who—
- (A) is not a health information trustee;
  - (B) is a contractor, subcontractor, associate, or subsidiary of a person who is a health information trustee; and
  - (C) pursuant to an agreement or other relationship with such trustee, receives, creates, uses, maintains, or discloses protected health information.
- (2) APPROVED HEALTH RESEARCH PROJECT.—The term “approved health research project” means a biomedical, epidemiological, or health services research or statistics project, or a research project on behavioral and social factors affecting health, that has been approved by a certified institutional review board.
- (3) CERTIFIED INSTITUTIONAL REVIEW BOARD.—The term “certified institutional review board” means a board—
- (A) established by an entity to review research involving protected health information and the rights of protected individuals conducted at or supported by the entity;
  - (B) established in accordance with regulations of the Secretary under section 116(d)(1); and
  - (C) certified by the Secretary under section 116(d)(2).
- (4) HEALTH CARE.—The term “health care”—
- (A) means—
    - (i) any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure—
      - (I) with respect to the physical or mental condition, or functional status, of an individual; or
      - (II) affecting the structure or function of the human body or any part of the human body, including banking of blood, sperm, organs, or any other tissue; or
    - (ii) any sale or dispensing of a drug, device, equipment, or other item to an individual, or for the use of an individual, pursuant to a prescription; but
  - (B) does not include any item or service that is not furnished for the purpose of maintaining or improving the health of an individual.
- (5) LAW ENFORCEMENT INQUIRY.—The term “law enforcement inquiry” means a lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant to such a statute.
- (6) PERSON.—The term “person” includes an authority of the United States, a State, or a political subdivision of a State.
- (7) SECRETARY.—The term “Secretary” means the Secretary of Health and Human Services.

(8) STATE.—The term “State” includes the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

## TITLE I—FAIR HEALTH INFORMATION PRACTICES

### Subtitle A—Duties of Health Information Trustees

#### SEC. 101. INSPECTION OF PROTECTED HEALTH INFORMATION.

(a) IN GENERAL.—Except as provided in subsection (b), a health information trustee described in subsection (g)—

(1) shall permit a protected individual to inspect any protected health information about the individual that the trustee maintains, any record with respect to such information required under section 104, and any copy of an authorization required under section 112 that pertains to such information;

(2) shall provide the protected individual with a copy of the information, upon request by the individual and subject to any conditions imposed by the trustee under subsection (d), in any form or format requested by the individual, if the information is readily reproducible by the trustee in such form or format;

(3) shall permit a person who has been designated in writing by the protected individual to inspect the information on behalf of the individual or to accompany the individual during the inspection; and

(4) may offer to explain or interpret information that is inspected or copied under this subsection.

(b) EXCEPTIONS.—A health information trustee is not required by this section to permit inspection or copying of protected health information by a protected individual if any of the following conditions apply:

(1) INFORMATION ABOUT OTHERS.—The information relates to an individual, other than the protected individual or a health care provider, and the trustee determines in the exercise of reasonable professional judgment that inspection or copying of the information would cause sufficient harm to one or both of the individuals so as to outweigh the desirability of permitting access.

(2) ENDANGERMENT TO LIFE OR SAFETY.—Inspection or copying of the information could reasonably be expected to endanger the life or physical safety of an individual.

(3) CONFIDENTIAL SOURCE.—The information identifies or could reasonably lead to the identification of an individual (other than a health care provider) who provided information under a promise of confidentiality to a health care provider concerning a protected individual who is a subject of the information.

(4) ADMINISTRATIVE PURPOSES.—The information—

(A) is used by the trustee solely for administrative purposes and not in the provision of health care to a protected individual who is a subject of the information; and

(B) is not disclosed by the trustee to any person.

(5) DUPLICATIVE INFORMATION.—The information duplicates information available for inspection under subsection (a).

(6) INFORMATION COMPILED IN ANTICIPATION OF LITIGATION.—The information is compiled principally—

(A) in anticipation of a civil, criminal, or administrative action or proceeding; or

(B) for use in such an action or proceeding.

(c) INSPECTION AND COPYING OF SEGREGABLE PORTION.—A health information trustee shall permit inspection and copying under subsection (a) of any reasonably segregable portion of a record after deletion of any portion that is exempt under subsection (b).

(d) CONDITIONS.—A health information trustee may—

(1) require a written request for the inspection and copying of protected health information under this section; and

(2) charge a reasonable cost-based fee for—

(A) permitting inspection of information under this section; and

(B) providing a copy of protected health information under this section.

(e) STATEMENT OF REASONS FOR DENIAL.—If a health information trustee denies in whole or in part a request for inspection or copying under this section, the trustee shall provide the protected individual who made the request with a written statement of the reasons for the denial.

(f) DEADLINE.—A health information trustee shall comply with or deny a request for inspection or copying of protected health information under this section within the 30-day period beginning on the date the trustee receives the request.

(g) **APPLICABILITY.**—This section applies to a health information trustee who is—

- (1) a health benefit plan sponsor;
- (2) a health care provider;
- (3) a health oversight agency; or
- (4) a public health authority.

**SEC. 102. AMENDMENT OF PROTECTED HEALTH INFORMATION.**

(a) **IN GENERAL.**—A health information trustee described in subsection (f) shall, within the 45-day period beginning on the date the trustee receives from a protected individual about whom the trustee maintains protected health information a written request that the trustee correct or amend the information, complete the duties described in one of the following paragraphs:

(1) **CORRECTION OR AMENDMENT AND NOTIFICATION.**—The trustee shall—

- (A) make the correction or amendment requested;
- (B) inform the protected individual of the amendment or correction that has been made;

(C) make reasonable efforts to inform any person who is identified by the protected individual, who is not an employee of the trustee, and to whom the uncorrected or unamended portion of the information was previously disclosed of the correction or amendment that has been made; and

(D) at the request of the individual, make reasonable efforts to inform any known source of the uncorrected or unamended portion of the information about the correction or amendment that has been made.

(2) **REASONS FOR REFUSAL AND REVIEW PROCEDURES.**—The trustee shall inform the protected individual of—

(A) the reasons for the refusal of the trustee to make the correction or amendment;

(B) any procedures for further review of the refusal; and

(C) the individual's right to file with the trustee a concise statement setting forth the requested correction or amendment and the individual's reasons for disagreeing with the refusal of the trustee.

(b) **STANDARDS FOR CORRECTION OR AMENDMENT.**—A trustee shall correct or amend protected health information in accordance with a request made under subsection (a) if the trustee determines that the information is not accurate, relevant, timely, or complete for the purposes for which the information may be used or disclosed by the trustee.

(c) **STATEMENT OF DISAGREEMENT.**—After a protected individual has filed a statement of disagreement under subsection (a)(2)(C), the trustee, in any subsequent disclosure of the disputed portion of the information, shall include a copy of the individual's statement and may include a concise statement of the trustee's reasons for not making the requested correction or amendment.

(d) **CONSTRUCTION.**—This section may not be construed to require a health information trustee to conduct a hearing or proceeding concerning a request for a correction or amendment to protected health information the trustee maintains.

(e) **CORRECTION.**—For purposes of subsection (a), a correction is deemed to have been made to protected health information when—

(1) information that is not timely, accurate, relevant, or complete is clearly marked as incorrect; or

(2) supplementary correct information is made part of the information and adequately cross-referenced.

(f) **APPLICABILITY.**—This section applies to a health information trustee who is—

- (1) a health benefit plan sponsor;
- (2) a health care provider;
- (3) a health oversight agency; or
- (4) a public health authority.

**SEC. 103. NOTICE OF INFORMATION PRACTICES.**

(a) **PREPARATION OF NOTICE.**—A health information trustee described in subsection (d) shall prepare a written notice of information practices describing the following:

(1) The rights under this Act of a protected individual who is the subject of protected health information, including the right to inspect and copy such information and the right to seek amendments to such information, and the procedures for authorizing disclosures of protected health information and for revoking such authorizations.

(2) The procedures established by the trustee for the exercise of such rights.

(3) The uses and disclosures of protected health information that are authorized under this Act.

(b) **DISSEMINATION OF NOTICE.**—A health information trustee—

(1) shall, upon request, provide any person with a copy of the trustee's notice of information practices (described in subsection (a)); and

(2) shall make reasonable efforts to inform persons in a clear and conspicuous manner of the existence and availability of such notice.

(c) **MODEL NOTICES.**—Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment, shall develop and disseminate model notices of information practices for use by health information trustees under this section.

(d) **APPLICABILITY.**—This section applies to a health information trustee who is—

- (1) a health benefit plan sponsor;
- (2) a health care provider; or
- (3) a health oversight agency.

**SEC. 104. DISCLOSURE HISTORY.**

(a) **IN GENERAL.**—Except as provided in subsection (b) and section 114, each health information trustee shall create and maintain, with respect to any protected health information the trustee discloses, a record of—

- (1) the date and purpose of the disclosure;
- (2) the name of the person to whom the disclosure was made;
- (3) the address of the person to whom the disclosure was made or the location to which the disclosure was made; and
- (4) where practicable, a description of the information disclosed.

(b) **REGULATIONS.**—Not later than July 1, 1999, the Secretary shall promulgate regulations that exempt a health information trustee from maintaining a record under subsection (a) with respect to protected health information disclosed by the trustee for purposes of peer review, licensing, certification, accreditation, and similar activities.

**SEC. 105. SECURITY.**

(a) **IN GENERAL.**—Each health information trustee who receives or creates protected health information that is subject to this Act shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

- (1) to ensure the integrity and confidentiality of the information;
- (2) to protect against any reasonably anticipated—
  - (A) threats or hazards to the security or integrity of the information; and
  - (B) unauthorized uses or disclosures of the information; and
- (3) otherwise ensure compliance with this Act by the trustee and the officers and employees of the trustee.

(b) **GUIDELINES.**—Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment, shall develop and disseminate guidelines for the implementation of this section. The guidelines shall take into account—

- (1) the technical capabilities of record systems used to maintain protected health information;
- (2) the costs of security measures;
- (3) the need for training persons who have access to protected health information; and
- (4) the value of audit trails in computerized record systems.

**Subtitle B—Use and Disclosure of Protected Health Information**

**SEC. 111. GENERAL LIMITATIONS ON USE AND DISCLOSURE.**

(a) **USE.**—Except as otherwise provided under this Act, a health information trustee may use protected health information only for a purpose—

- (1) that is compatible with and directly related to the purpose for which the information—
  - (A) was collected; or
  - (B) was received by the trustee; or
- (2) for which the trustee is authorized to disclose the information under this Act.

(b) **DISCLOSURE.**—A health information trustee may disclose protected health information only as authorized under this Act.

(c) **SCOPE OF USES AND DISCLOSURES.**—

- (1) **IN GENERAL.**—A use or disclosure of protected health information by a health information trustee shall be limited, when practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

(2) **GUIDELINES.**—Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment, shall issue guidelines to implement paragraph (1), which shall take into account the technical capabilities of the record systems used to maintain protected health information and the costs of limiting use and disclosure.

(d) **IDENTIFICATION OF DISCLOSED INFORMATION AS PROTECTED INFORMATION.**—Except with respect to protected health information that is disclosed under section 114 (relating to next of kin and directory information), a health information trustee may disclose protected health information only if the recipient has been notified that the information is protected health information that is subject to this Act.

(e) **AGREEMENT TO LIMIT USE OR DISCLOSURE.**—A health information trustee who receives protected health information from any person pursuant to a written agreement to restrict use or disclosure of the information to a greater extent than otherwise would be required under this Act shall comply with the terms of the agreement, except where use or disclosure of the information in violation of the agreement is required by law. A trustee who fails to comply with the preceding sentence shall be subject to section 151 (relating to civil actions) with respect to such failure.

(f) **NO GENERAL REQUIREMENT TO DISCLOSE.**—Nothing in this Act shall be construed to require a health information trustee to disclose protected health information not otherwise required to be disclosed by law.

**SEC. 112. AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION.**

(a) **WRITTEN AUTHORIZATIONS.**—A health information trustee may disclose protected health information pursuant to an authorization executed by the protected individual who is the subject of the information, if each of the following requirements is satisfied:

(1) **WRITING.**—The authorization is in writing, signed by the individual, and dated on the date of such signature.

(2) **SEPARATE FORM.**—The authorization is not on a form used to authorize or facilitate the provision of, or payment for, health care.

(3) **TRUSTEE DESCRIBED.**—The trustee is specifically named or generically described in the authorization as authorized to disclose such information.

(4) **RECIPIENT DESCRIBED.**—The person to whom the information is to be disclosed is specifically named or generically described in the authorization as a person to whom such information may be disclosed.

(5) **STATEMENT OF INTENDED USES AND DISCLOSURES RECEIVED.**—The authorization contains an acknowledgment that the individual has received a statement described in subsection (b) from such person.

(6) **INFORMATION DESCRIBED.**—The information to be disclosed is described in the authorization.

(7) **AUTHORIZATION TIMELY RECEIVED.**—The authorization is received by the trustee during a period described in subsection (c)(1).

(8) **DISCLOSURE TIMELY MADE.**—The disclosure occurs during a period described in subsection (c)(2).

(b) **STATEMENT OF INTENDED USES AND DISCLOSURES.**—

(1) **IN GENERAL.**—A person who wishes to receive from a health information trustee protected health information about a protected individual pursuant to an authorization executed by the individual shall supply the individual, in writing and on a form that is distinct from the authorization, with a statement of the uses for which the person intends the information and the disclosures the person intends to make of the information. Such statement shall be supplied before the authorization is executed.

(2) **ENFORCEMENT.**—If the person uses or discloses the information in a manner that is inconsistent with such statement, the person shall be subject to section 151 (relating to civil actions) with respect to such failure, except where such use or disclosure is required by law.

(3) **MODEL STATEMENTS.**—Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment, shall develop and disseminate model statements of intended uses and disclosures of the type described in paragraph (1).

(c) **TIME LIMITATIONS ON AUTHORIZATIONS.**—

(1) **RECEIPT BY TRUSTEE.**—For purposes of subsection (a)(7), an authorization is timely received if it is received by the trustee during—

(A) the 1-year period beginning on the date that the authorization is signed under subsection (a)(1), if the authorization permits the disclosure of protected health information to—

(i) a health benefit plan sponsor;

- (ii) a health care provider;
  - (iii) a health oversight agency;
  - (iv) a public health authority;
  - (v) a health researcher; or
  - (vi) a person who provides counseling or social services to individuals; or
  - (B) the 30-day period beginning on the date that the authorization is signed under subsection (a)(1), if the authorization permits the disclosure of protected health information to a person other than a person described in subparagraph (A).
- (2) DISCLOSURE BY TRUSTEE.—For purposes of subsection (a)(8), a disclosure is timely made if it occurs before—
- (A) the date or event (if any) specified in the authorization upon which the authorization expires; and
  - (B) the expiration of the 6-month period beginning on the date the trustee receives the authorization.
- (d) REVOCATION OR AMENDMENT OF AUTHORIZATION.—
- (1) IN GENERAL.—A protected individual in writing may revoke or amend an authorization described in subsection (a), in whole or in part, at any time, except insofar as—
- (A) disclosure of protected health information has been authorized to permit validation of expenditures based on health condition by a government authority; or
  - (B) action has been taken in reliance on the authorization.
- (2) NOTICE OF REVOCATION.—A health information trustee who discloses protected health information in reliance on an authorization that has been revoked shall not be subject to any liability or penalty under this Act if—
- (A) the reliance was in good faith;
  - (B) the trustee had no notice of the revocation; and
  - (C) the disclosure was otherwise in accordance with the requirements of this section.
- (e) ADDITIONAL REQUIREMENTS OF TRUSTEE.—A health information trustee may impose requirements for an authorization that are in addition to the requirements in this section.
- (f) COPY.—A health information trustee who discloses protected health information pursuant to an authorization under this section shall maintain a copy of the authorization.
- (g) CONSTRUCTION.—This section may not be construed—
- (1) to require a health information trustee to disclose protected health information; or
  - (2) to limit the right of a health information trustee to charge a fee for the disclosure or reproduction of protected health information.
- (h) SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.—If a health information trustee discloses protected health information pursuant to an authorization in order to comply with an administrative subpoena or warrant or a judicial subpoena or search warrant, the authorization—
- (1) shall specifically authorize the disclosure for the purpose of permitting the trustee to comply with the subpoena, warrant, or search warrant; and
  - (2) shall otherwise meet the requirements in this section.

**SEC. 113. TREATMENT, PAYMENT, AND OVERSIGHT.**

- (a) DISCLOSURES BY PLANS, PROVIDERS, AND OVERSIGHT AGENCIES.—A health information trustee described in subsection (d) may disclose protected health information to a health benefit plan sponsor, health care provider, or health oversight agency if the disclosure is—
- (1) for the purpose of providing health care and a protected individual who is a subject of the information has not previously objected to the disclosure in writing;
  - (2) for the purpose of providing for the payment for health care furnished to an individual; or
  - (3) for use by a health oversight agency for a purpose that is described in subparagraph (A) or (B)(i) of section 3(b)(6).
- (b) DISCLOSURES BY CERTAIN OTHER TRUSTEES.—A health information trustee may disclose protected health information to a health care provider if—
- (1) the disclosure is for the purpose described in subsection (a)(1); and
  - (2) the trustee—
    - (A) is a public health authority;

(B) received protected health information pursuant to section 117 (relating to emergency circumstances); or

(C) is an officer or employee of a trustee described in subparagraph (B).

(c) **USE IN ACTION AGAINST INDIVIDUAL.**—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and related to receipt of health care or payment for health care.

(d) **APPLICABILITY.**—A health information trustee referred to in subsection (a) is any of the following:

- (1) A health benefit plan sponsor.
- (2) A health care provider.
- (3) A health oversight agency.

**SEC. 114. NEXT OF KIN AND DIRECTORY INFORMATION.**

(a) **NEXT OF KIN.**—A health information trustee who is a health care provider, who received protected health information pursuant to section 117 (relating to emergency circumstances), or who is an officer or employee of such a recipient may orally disclose protected health information about a protected individual to the next of kin of the individual (as defined under State law), or to a person with whom the individual has a close personal relationship, if—

- (1) the trustee has no reason to believe that the individual would consider the information especially sensitive;
- (2) the individual has not previously objected to the disclosure;
- (3) the disclosure is consistent with good medical or other professional practice; and

(4) the information disclosed is limited to information about health care that is being provided to the individual at or about the time of the disclosure.

(b) **DIRECTORY INFORMATION.**—

(1) **IN GENERAL.**—A health information trustee who is a health care provider, who received protected health information pursuant to section 117 (relating to emergency circumstances), or who is an officer or employee of such a recipient may disclose to any person the information described in paragraph (2) if—

- (A) a protected individual who is a subject of the information has not objected in writing to the disclosure;
- (B) the disclosure is otherwise consistent with good medical and other professional practice; and
- (C) the information does not reveal specific information about the physical or mental condition or functional status of a protected individual or about the health care provided to a protected individual.

(2) **INFORMATION DESCRIBED.**—The information referred to in paragraph (1) is the following:

- (A) The name of an individual receiving health care from a health care provider on a premises controlled by the provider.
- (B) The location of the individual on such premises.
- (C) The general health status of the individual, described in terms of critical, poor, fair, stable, satisfactory, or terms denoting similar conditions.

(c) **NO DISCLOSURE RECORD REQUIRED.**—A health information trustee who discloses protected health information under this section is not required to create and maintain a record of the disclosure under section 104.

(d) **RECIPIENTS.**—A person to whom protected health information is disclosed under this section shall not, by reason of such disclosure, be subject to any requirement under this Act.

**SEC. 115. PUBLIC HEALTH.**

(a) **IN GENERAL.**—A health information trustee who is a health care provider or a public health authority may disclose protected health information to—

- (1) a public health authority for use in legally authorized—
  - (A) disease or injury reporting;
  - (B) public health surveillance; or
  - (C) public health investigation or intervention; or

(2) an individual who is authorized by law to receive the information in a public health intervention.

(b) **USE IN ACTION AGAINST INDIVIDUAL.**—A public health authority who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except where the use or disclosure is authorized by law for protection of the public health.

(c) **INDIVIDUAL RECIPIENTS.**—An individual to whom protected health information is disclosed under subsection (a)(2) shall not, by reason of such disclosure, be subject to any requirement under this Act.

**SEC. 116. HEALTH RESEARCH.**

(a) **IN GENERAL.**—A health information trustee described in subsection (c) may disclose protected health information to a person if—

- (1) the person is conducting an approved health research project;
- (2) the information is to be used in the project; and

(3) the project has been determined by a certified institutional review board to be—

(A) of sufficient importance so as to outweigh the intrusion into the privacy of the protected individual who is the subject of the information that would result from the disclosure; and

(B) impracticable to conduct without the information.

(b) **LIMITATIONS ON USE AND DISCLOSURE; OBLIGATIONS OF RECIPIENT.**—A health researcher who receives protected health information about a protected individual pursuant to subsection (a)—

(1) may use the information solely for purposes of an approved health research project;

(2) may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual; and

(3) shall remove or destroy, at the earliest opportunity consistent with the purposes of the approved health research project in connection with which the disclosure was made, information that would enable an individual to be identified, unless a certified institutional review board has determined that there is a health or research justification for retention of such identifiers and there is an adequate plan to protect the identifiers from use and disclosure that is inconsistent with this Act.

(c) **APPLICABILITY.**—A health information trustee referred to in subsection (a) is any health information trustee other than a person who, with respect to the specific protected health information to be disclosed under such subsection, received the information—

(1) pursuant to—

(A) section 118 (relating to judicial and administrative purposes);

(B) paragraph (1), (2), (3), or (4) of section 119(a) (relating to law enforcement); or

(C) section 120 (relating to subpoenas, warrants, and search warrants);

or

(2) while acting in whole or in part in the capacity of an officer or employee of a person described in paragraph (1).

(d) **REQUIREMENTS FOR INSTITUTIONAL REVIEW BOARDS.**—

(1) **REGULATIONS.**—Not later than July 1, 1999, the Secretary, after opportunity for notice and comment, shall promulgate regulations establishing requirements for certified institutional review boards under this Act. The regulations shall be based on regulations promulgated under section 491(a) of the Public Health Service Act and shall ensure that certified institutional review boards are qualified to assess and protect the confidentiality of research subjects.

(2) **CERTIFICATION.**—The Secretary shall certify that an institutional review board satisfies the requirements of the regulations promulgated under paragraph (1).

**SEC. 117. EMERGENCY CIRCUMSTANCES.**

(a) **IN GENERAL.**—A health information trustee may disclose protected health information if the trustee believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual.

(b) **USE IN ACTION AGAINST INDIVIDUAL.**—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and related to receipt of health care or payment for health care.

**SEC. 118. JUDICIAL AND ADMINISTRATIVE PURPOSES.**

(a) **IN GENERAL.**—A health information trustee described in subsection (d) may disclose protected health information—

(1) pursuant to the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, or comparable rules of other courts or administrative agen-

cies in connection with litigation or proceedings to which a protected individual who is a subject of the information is a party and in which the individual has placed the individual's physical or mental condition or functional status in issue;

(2) if directed by a court in connection with a court-ordered examination of an individual; or

(3) to assist in the identification of a dead individual.

(b) **WRITTEN STATEMENT.**—A person seeking protected health information about a protected individual held by health information trustee under—

(1) subsection (a)(1)—

(A) shall notify the protected individual or the attorney of the protected individual of the request for the information;

(B) shall provide the trustee with a signed document attesting—

(i) that the protected individual is a party to the litigation or proceedings for which the information is sought;

(ii) that the individual has placed the individual's physical or mental condition or functional status in issue; and

(iii) the date on which the protected individual or the attorney of the protected individual was notified under subparagraph (A); and

(C) shall not accept any requested protected health information from the trustee until the termination of the 10-day period beginning on the date notice was given under subparagraph (A); or

(2) subsection (a)(3) shall provide the trustee with a written statement that the information is sought to assist in the identification of a dead individual.

(c) **USE AND DISCLOSURE.**—A person to whom protected health information is disclosed under this section may use and disclose the information only to accomplish the purpose for which the disclosure was made.

(d) **APPLICABILITY.**—A health information trustee referred to in subsection (a) is any of the following:

(1) A health benefit plan sponsor.

(2) A health care provider.

(3) A health oversight agency.

(4) A person who, with respect to the specific protected health information to be disclosed under such subsection, received the information—

(A) pursuant to—

(i) section 117 (relating to emergency circumstances); or

(ii) section 120 (relating to subpoenas, warrants, and search warrants); or

(B) while acting in whole or in part in the capacity of an officer or employee of a person described in subparagraph (A).

#### **SEC. 119. LAW ENFORCEMENT.**

(a) **IN GENERAL.**—A health information trustee may disclose protected health information to a law enforcement agency, other than a health oversight agency—

(1) if the information is disclosed for use in an investigation or prosecution of a health information trustee;

(2) in connection with criminal activity committed against the trustee or an affiliated person of the trustee or on premises controlled by the trustee; or

(3) if the information is needed to determine whether a crime has been committed and the nature of any crime that may have been committed (other than a crime that may have been committed by the protected individual who is the subject of the information).

(b) **ADDITIONAL AUTHORITY OF CERTAIN TRUSTEES.**—A health information trustee who is not a public health authority or a health researcher may disclose protected health information to a law enforcement agency (other than a health oversight agency)—

(1) to assist in the identification or location of a victim, fugitive, or witness in a law enforcement inquiry;

(2) pursuant to a law requiring the reporting of specific health care information to law enforcement authorities; or

(3) if the information is specific health information described in paragraph (2) and the trustee is operated by a Federal agency;

(c) **CERTIFICATION.**—Where a law enforcement agency requests a health information trustee to disclose protected health information under subsection (a) or (b)(1), the agency shall provide the trustee with a written certification that—

(1) is signed by a supervisory official of a rank designated by the head of the agency;

(2) specifies the information requested; and

(3) states that the information is needed for a lawful purpose under this section.

(d) **RESTRICTIONS ON DISCLOSURE AND USE.**—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information—

(1) in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and directly related to the action or investigation for which the information was obtained; and

(2) otherwise unless the use or disclosure is necessary to fulfill the purpose for which the information was obtained and is not prohibited by any other provision of law.

**SEC. 120. SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.**

(a) **IN GENERAL.**—A health information trustee described in subsection (g) may disclose protected health information if the disclosure is pursuant to any of the following:

(1) A subpoena issued under the authority of a grand jury and the trustee is provided a written certification by the grand jury that the grand jury has complied with the applicable access provisions of section 131.

(2) An administrative subpoena or warrant or a judicial subpoena or search warrant and the trustee is provided a written certification by the person seeking the information that the person has complied with the applicable access provisions of section 131 or 133(a).

(3) An administrative subpoena or warrant or a judicial subpoena or search warrant and the disclosure otherwise meets the conditions of one of sections 113 through 119.

(b) **AUTHORITY OF ALL TRUSTEES.**—Any health information trustee may disclose protected health information if the disclosure is pursuant to subsection (a)(3).

(c) **RESTRICTIONS ON USE AND DISCLOSURE.**—Protected health information about a protected individual that is disclosed by a health information trustee pursuant to—

(1) subsection (a)(2) may not be otherwise used or disclosed by the recipient unless the use or disclosure is necessary to fulfill the purpose for which the information was obtained; and

(2) subsection (a)(3) may not be used or disclosed by the recipient unless the recipient complies with the conditions and restrictions on use and disclosure with which the recipient would have been required to comply if the disclosure by the trustee had been made under the section referred to in subsection (a)(3) the conditions of which were met by the disclosure.

(d) **RESTRICTIONS ON GRAND JURIES.**—Protected health information that is disclosed by a health information trustee under subsection (a)(1)—

(1) shall be returnable on a date when the grand jury is in session and actually presented to the grand jury;

(2) shall be used only for the purpose of considering whether to issue an indictment or report by that grand jury, or for the purpose of prosecuting a crime for which that indictment or report is issued, or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure or a comparable State rule;

(3) shall be destroyed or returned to the trustee if not used for one of the purposes specified in paragraph (2); and

(4) shall not be maintained, or a description of the contents of such information shall not be maintained, by any government authority other than in the sealed records of the grand jury, unless such information has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure or a comparable State rule.

(e) **USE IN ACTION AGAINST INDIVIDUAL.**—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and directly related to the inquiry for which the information was obtained;

(f) **CONSTRUCTION.**—Nothing in this section shall be construed as authority for a health information trustee to refuse to comply with a valid administrative subpoena or warrant or a valid judicial subpoena or search warrant that meets the requirements of this Act.

(g) **APPLICABILITY.**—A health information trustee referred to in subsection (a) is any trustee other than the following:

- (1) A public health authority.
- (2) A health researcher.

### **Subtitle C—Access Procedures and Challenge Rights**

#### **SEC. 131. ACCESS PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.**

(a) **PROBABLE CAUSE REQUIREMENT.**—A government authority may not obtain protected health information about a protected individual from a health information trustee under paragraph (1) or (2) of section 120(a) for use in a law enforcement inquiry unless there is probable cause to believe that the information is relevant to a legitimate law enforcement inquiry being conducted by the government authority.

(b) **WARRANTS AND SEARCH WARRANTS.**—A government authority that obtains protected health information about a protected individual from a health information trustee under circumstances described in subsection (a) and pursuant to a warrant or search warrant shall, not later than 30 days after the date the warrant was served on the trustee, serve the individual with, or mail to the last known address of the individual, a copy of the warrant.

(c) **SUBPOENAS.**—Except as provided in subsection (d), a government authority may not obtain protected health information about a protected individual from a health information trustee under circumstances described in subsection (a) and pursuant to a subpoena unless a copy of the subpoena has been served by hand delivery upon the individual, or mailed to the last known address of the individual, on or before the date on which the subpoena was served on the trustee, together with a notice (published by the Secretary under section 135(1)) of the individual’s right to challenge the subpoena in accordance with section 132, and—

(1) 30 days have passed from the date of service, or 30 days have passed from the date of mailing, and within such time period the individual has not initiated a challenge in accordance with section 132; or

(2) disclosure is ordered by a court under section 132.

(d) **APPLICATION FOR DELAY.**—

(1) **IN GENERAL.**—A government authority may apply to an appropriate court to delay (for an initial period of not longer than 90 days) serving a copy of a subpoena and a notice otherwise required under subsection (c) with respect to a law enforcement inquiry. The government authority may apply to the court for extensions of the delay.

(2) **REASONS FOR DELAY.**—An application for a delay, or extension of a delay, under this subsection shall state, with reasonable specificity, the reasons why the delay or extension is being sought.

(3) **EX PARTE ORDER.**—The court shall enter an ex parte order delaying, or extending the delay of, the notice and an order prohibiting the trustee from revealing the request for, or the disclosure of, the protected health information being sought if the court finds that—

(A) the inquiry being conducted is within the lawful jurisdiction of the government authority seeking the protected health information;

(B) there is probable cause to believe that the protected health information being sought is relevant to a legitimate law enforcement inquiry being conducted by the government authority;

(C) the government authority’s need for the information outweighs the privacy interest of the protected individual who is the subject of the information; and

(D) there are reasonable grounds to believe that receipt of a notice by the individual will result in—

(i) endangering the life or physical safety of any individual;

(ii) flight from prosecution;

(iii) destruction of or tampering with evidence or the information being sought; or

(iv) intimidation of potential witnesses.

(4) **SERVICE OF APPLICATION ON INDIVIDUAL.**—Upon the expiration of a period of delay of notice under this subsection, the government authority shall serve upon the individual, with the service of the subpoena and the notice, a copy of any applications filed and approved under this subsection.

#### **SEC. 132. CHALLENGE PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS.**

(a) **MOTION TO QUASH SUBPOENA.**—Within 30 days of the date of service, or 30 days of the date of mailing, of a subpoena of a government authority seeking pro-

tected health information about a protected individual from a health information trustee under paragraph (1) or (2) of section 120(a) (except a subpoena to which section 133 applies), the individual may file (without filing fee) a motion to quash the subpoena—

(1) in the case of a State judicial subpoena, in the court which issued the subpoena;

(2) in the case of a subpoena issued under the authority of a State that is not a State judicial subpoena, in a court of competent jurisdiction;

(3) in the case of a subpoena issued under the authority of a Federal court, in any court of the United States of competent jurisdiction; or

(4) in the case of any other subpoena issued under the authority of the United States, in—

(A) the United States district court for the district in which the individual resides or in which the subpoena was issued; or

(B) another United States district court of competent jurisdiction.

(b) COPY.—A copy of the motion shall be served by the individual upon the government authority by delivery of registered or certified mail.

(c) AFFIDAVITS AND SWORN DOCUMENTS.—The government authority may file with the court such affidavits and other sworn documents as sustain the validity of the subpoena. The individual may file with the court, within 5 days of the date of the authority's filing, affidavits and sworn documents in response to the authority's filing. The court, upon the request of the individual, the government authority, or both, may proceed in camera.

(d) PROCEEDINGS AND DECISION ON MOTION.—The court may conduct such proceedings as it deems appropriate to rule on the motion. All such proceedings shall be completed, and the motion ruled on, within 10 calendar days of the date of the government authority's filing.

(e) EXTENSION OF TIME LIMITS FOR GOOD CAUSE.—The court, for good cause shown, may at any time in its discretion enlarge the time limits established by subsections (c) and (d).

(f) STANDARD FOR DECISION.—A court may deny a motion under subsection (a) if it finds that there is probable cause to believe that the protected health information being sought is relevant to a legitimate law enforcement inquiry being conducted by the government authority, unless the court finds that the individual's privacy interest outweighs the government authority's need for the information. The individual shall have the burden of demonstrating that the individual's privacy interest outweighs the need established by the government authority for the information.

(g) SPECIFIC CONSIDERATIONS WITH RESPECT TO PRIVACY INTEREST.—In determining under subsection (f) whether an individual's privacy interest outweighs the government authority's need for the information, the court shall consider—

(1) the particular purpose for which the information was collected by the trustee;

(2) the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the individual;

(3) the effect of the disclosure on the individual's future health care;

(4) the importance of the inquiry being conducted by the government authority, and the importance of the information to that inquiry; and

(5) any other factor deemed relevant by the court.

(h) ATTORNEY'S FEES.—In the case of any motion brought under subsection (a) in which the individual has substantially prevailed, the court, in its discretion, may assess against a government authority a reasonable attorney's fee and other litigation costs (including expert fees) reasonably incurred.

(i) NO INTERLOCUTORY APPEAL.—A court ruling denying a motion to quash under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the individual. An appeal of such a ruling may be taken by the individual within such period of time as is provided by law as part of any appeal from a final order in any legal proceeding initiated against the individual arising out of or based upon the protected health information disclosed.

#### SEC. 133. ACCESS AND CHALLENGE PROCEDURES FOR OTHER SUBPOENAS.

(a) IN GENERAL.—A person (other than a government authority seeking protected health information under circumstances described in section 131(a)) may not obtain protected health information about a protected individual from a health information trustee pursuant to a subpoena under section 120(a)(2) unless—

(1) a copy of the subpoena has been served upon the individual or mailed to the last known address of the individual on or before the date on which the subpoena was served on the trustee, together with a notice (published by the

Secretary under section 135(2) of the individual's right to challenge the subpoena, in accordance with subsection (b); and

(2) either—

(A) 30 days have passed from the date of service or 30 days have passed from the date of the mailing and within such time period the individual has not initiated a challenge in accordance with subsection (b); or

(B) disclosure is ordered by a court under such subsection.

(b) **MOTION TO QUASH.**—Within 30 days of the date of service or 30 days of the date of mailing of a subpoena seeking protected health information about a protected individual from a health information trustee under subsection (a), the individual may file (without filing fee) in any court of competent jurisdiction, a motion to quash the subpoena, with a copy served on the person seeking the information. The individual may oppose, or seek to limit, the subpoena on any grounds that would otherwise be available if the individual were in possession of the information.

(c) **STANDARD FOR DECISION.**—The court shall grant an individual's motion under subsection (b) if the person seeking the information has not sustained the burden of demonstrating that—

(1) there are reasonable grounds to believe that the information will be relevant to a lawsuit or other judicial or administrative proceeding; and

(2) the need of the person for the information outweighs the privacy interest of the individual.

(d) **SPECIFIC CONSIDERATIONS WITH RESPECT TO PRIVACY INTEREST.**—In determining under subsection (c) whether the need of the person for the information outweighs the privacy interest of the individual, the court shall consider—

(1) the particular purpose for which the information was collected by the trustee;

(2) the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the individual;

(3) the effect of the disclosure on the individual's future health care;

(4) the importance of the information to the lawsuit or proceeding; and

(5) any other factor deemed relevant by the court.

(e) **ATTORNEY'S FEES.**—In the case of any motion brought under subsection (b) by an individual against a person in which the individual has substantially prevailed, the court, in its discretion, may assess against the person a reasonable attorney's fee and other litigation costs (including expert fees) reasonably incurred.

**SEC. 134. CONSTRUCTION OF SUBTITLE; SUSPENSION OF STATUTE OF LIMITATIONS.**

(a) **IN GENERAL.**—Nothing in this subtitle shall affect the right of a health information trustee to challenge a request for protected health information. Nothing in this subtitle shall entitle a protected individual to assert the rights of a health information trustee.

(b) **EFFECT OF MOTION ON STATUTE OF LIMITATIONS.**—If an individual who is the subject of protected health information files a motion under this subtitle which has the effect of delaying the access of a government authority to such information, the period beginning on the date such motion was filed and ending on the date on which the motion is decided shall be excluded in computing any period of limitations within which the government authority may commence any civil or criminal action in connection with which the access is sought.

**SEC. 135. RESPONSIBILITIES OF SECRETARY.**

Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment, shall develop and disseminate brief, clear, and easily understood model notices—

(1) for use under subsection (c) of section 131, detailing the rights of a protected individual who wishes to challenge, under section 132, the disclosure of protected health information about the individual under such subsection; and

(2) for use under subsection (a) of section 133, detailing the rights of a protected individual who wishes to challenge, under subsection (b) of such section, the disclosure of protected health information about the individual under such section.

**Subtitle D—Miscellaneous Provisions**

**SEC. 141. PAYMENT CARD AND ELECTRONIC PAYMENT TRANSACTIONS.**

(a) **PAYMENT FOR HEALTH CARE THROUGH CARD OR ELECTRONIC MEANS.**—If a protected individual pays a health information trustee for health care by presenting a debit, credit, or other payment card or account number, or by any other electronic payment means, the trustee may disclose to a person described in subsection (b) only such protected health information about the individual as is necessary for the

processing of the payment transaction or the billing or collection of amounts charged to, debited from, or otherwise paid by, the individual using the card, number, or other electronic payment means.

(b) TRANSACTION PROCESSING.—A person who is a debit, credit, or other payment card issuer, is otherwise directly involved in the processing of payment transactions involving such cards or other electronic payment transactions, or is otherwise directly involved in the billing or collection of amounts paid through such means, may only use or disclose protected health information about a protected individual that has been disclosed in accordance with subsection (a) when necessary for—

- (1) the authorization, settlement, billing or collection of amounts charged to, debited from, or otherwise paid by, the individual using a debit, credit, or other payment card or account number, or by other electronic payment means;
- (2) the transfer of receivables, accounts, or interest therein;
- (3) the audit of the credit, debit, or other payment card account information;
- (4) compliance with Federal, State, or local law; or
- (5) a properly authorized civil, criminal, or regulatory investigation by Federal, State, or local authorities.

**SEC. 142. ACCESS TO PROTECTED HEALTH INFORMATION OUTSIDE OF THE UNITED STATES.**

(a) IN GENERAL.—Notwithstanding the provisions of subtitle B, and except as provided in subsection (b), a health information trustee may not permit any person who is not in a State to have access to protected health information about a protected individual unless one or more of the following conditions exist:

- (1) SPECIFIC AUTHORIZATION.—The individual has specifically consented to the provision of such access outside of the United States in an authorization that meets the requirements of section 112.
- (2) EQUIVALENT PROTECTION.—The provision of such access is authorized under this Act and the Secretary has determined that there are fair information practices for protected health information in the jurisdiction where the access will be provided that provide protections for individuals and protected health information that are equivalent to the protections provided for by this Act.

(3) ACCESS REQUIRED BY LAW.—The provision of such access is required under—

- (A) a Federal statute; or
- (B) a treaty or other international agreement applicable to the United States.

(b) EXCEPTIONS.—Subsection (a) does not apply where the provision of access to protected health information—

- (1) is to a foreign public health authority;
- (2) is authorized under section 114 (relating to next of kin and directory information), 116 (relating to health research), or 117 (relating to emergency circumstances); or
- (3) is necessary for the purpose of providing for payment for health care that has been provided to an individual.

**SEC. 143. STANDARDS FOR ELECTRONIC DOCUMENTS AND COMMUNICATIONS.**

(a) STANDARDS.—Not later than July 1, 1999, the Secretary, after notice and opportunity for public comment and in consultation with appropriate private standard-setting organizations and other interested parties, shall establish standards with respect to the creation, transmission, receipt, and maintenance, in electronic and magnetic form, of each type of written document specifically required or authorized under this Act. Where a signature is required under any other provision of this Act, such standards shall provide for an electronic or magnetic substitute that serves the functional equivalent of a signature.

(b) TREATMENT OF COMPLYING DOCUMENTS AND COMMUNICATIONS.—An electronic or magnetic document or communication that satisfies the standards established under subsection (a) with respect to such document or communication shall be treated as satisfying the requirements of this Act that apply to an equivalent written document.

**SEC. 144. DUTIES AND AUTHORITIES OF AFFILIATED PERSONS.**

(a) REQUIREMENTS ON TRUSTEES.—

- (1) PROVISION OF INFORMATION.—A health information trustee may provide protected health information to a person who, with respect to the trustee, is an affiliated person and may permit the affiliated person to use such information, only for the purpose of conducting, supporting, or facilitating an activity that the trustee is authorized to undertake.

(2) NOTICE TO AFFILIATED PERSON.—A health information trustee shall notify a person who, with respect to the trustee, is an affiliated person of any duties under this Act that the affiliated person is required to fulfill and of any authorities under this Act that the affiliated person is authorized to exercise.

(b) DUTIES OF AFFILIATED PERSONS.—

(1) IN GENERAL.—An affiliated person shall fulfill any duty under this Act that—

(A) the health information trustee with whom the person has an agreement or relationship described in section 3(c)(1)(C) is required to fulfill; and

(B) the person has undertaken to fulfill pursuant to such agreement or relationship.

(2) CONSTRUCTION OF OTHER SUBTITLES.—With respect to a duty described in paragraph (1) that an affiliated person is required to fulfill, the person shall be considered a health information trustee for purposes of this Act. The person shall be subject to subtitle E (relating to enforcement) with respect to any such duty that the person fails to fulfill.

(3) EFFECT ON TRUSTEE.—An agreement or relationship with an affiliated person does not relieve a health information trustee of any duty or liability under this Act.

(b) AUTHORITIES OF AFFILIATED PERSONS.—

(1) IN GENERAL.—An affiliated person may only exercise an authority under this Act that the health information trustee with whom the person is affiliated may exercise and that the person has been given by the trustee pursuant to an agreement or relationship described in section 3(c)(1)(C). With respect to any such authority, the person shall be considered a health information trustee for purposes of this Act. The person shall be subject to subtitle E (relating to enforcement) with respect to any act that exceeds such authority.

(2) EFFECT ON TRUSTEE.—An agreement or relationship with an affiliated person does not affect the authority of a health information trustee under this Act.

#### SEC. 145. AGENTS AND ATTORNEYS.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), a person who is authorized by law (on grounds other than an individual's minority), or by an instrument recognized under law, to act as an agent, attorney, proxy, or other legal representative for a protected individual or the estate of a protected individual, or otherwise to exercise the rights of the individual or estate, may, to the extent authorized, exercise and discharge the rights of the individual or estate under this Act.

(b) HEALTH CARE POWER OF ATTORNEY.—A person who is authorized by law (on grounds other than an individual's minority), or by an instrument recognized under law, to make decisions about the provision of health care to an individual who is incapacitated may exercise and discharge the rights of the individual under this Act to the extent necessary to effectuate the terms or purposes of the grant of authority.

(c) NO COURT DECLARATION.—If a health care provider determines that an individual, who has not been declared to be legally incompetent, suffers from a medical condition that prevents the individual from acting knowingly or effectively on the individual's own behalf, the right of the individual to authorize disclosure under section 112 may be exercised and discharged in the best interest of the individual by—

(1) a person described in subsection (b) with respect to the individual;

(2) a person described in subsection (a) with respect to the individual, but only if a person described in paragraph (1) cannot be contacted after a reasonable effort;

(3) the next of kin of the individual, but only if a person described in paragraph (1) or (2) cannot be contacted after a reasonable effort; or

(4) the health care provider, but only if a person described in paragraph (1), (2), or (3) cannot be contacted after a reasonable effort.

#### SEC. 146. MINORS.

(a) INDIVIDUALS WHO ARE 18 OR LEGALLY CAPABLE.—In the case of an individual—

(1) who is 18 years of age or older, all rights of the individual shall be exercised by the individual, except as provided in section 145; or

(2) who, acting alone, has the legal capacity to apply for and obtain health care and has sought such care, the individual shall exercise all rights of an individual under this Act with respect to protected health information relating to such care.

(b) INDIVIDUALS UNDER 18.—Except as provided in subsection (a)(2), in the case of an individual who is—

(1) under 14 years of age, all the individual's rights under this Act shall be exercised through the parent or legal guardian of the individual; or

(2) 14, 15, 16, or 17 years of age, the right of inspection (under section 101), the right of amendment (under section 102), and the right to authorize disclosure of protected health information (under section 112) of the individual may be exercised either by the individual or by the parent or legal guardian of the individual.

**SEC. 147. MAINTENANCE OF CERTAIN PROTECTED HEALTH INFORMATION.**

(a) **IN GENERAL.**—A State shall establish a process under which the protected health information described in subsection (b) that is maintained by a person described in subsection (c) is delivered to, and maintained by, the State or an individual or entity designated by the State.

(b) **INFORMATION DESCRIBED.**—The protected health information referred to in subsection (a) is protected health information that—

(1) is recorded in any form or medium;

(2) is created by—

(A) a health care provider; or

(B) a health benefit plan sponsor that provides benefits in the form of items and services to enrollees and not in the form of reimbursement for items and services; and

(3) relates in any way to the past, present, or future physical or mental health or condition or functional status of a protected individual or the provision of health care to a protected individual.

(c) **PERSONS DESCRIBED.**—A person referred to in subsection (a) is any of the following:

(1) A health care facility previously located in the State that has closed.

(2) A professional practice previously operated by a health care provider in the State that has closed.

(3) A health benefit plan sponsor that—

(A) previously provided benefits in the form of items and services to enrollees in the State; and

(B) has ceased to do business.

**Subtitle E—Enforcement**

**SEC. 151. CIVIL ACTIONS.**

(a) **IN GENERAL.**—Any individual whose right under this Act has been knowingly or negligently violated—

(1) by a health information trustee, or any other person, who is not described in paragraph (2), (3), (4), or (5) may maintain a civil action for actual damages and for equitable relief against the health information trustee or other person;

(2) by an officer or employee of the United States while the officer or employee was acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the United States;

(3) by an officer or employee of any government authority of a State that has waived its sovereign immunity to a claim for damages resulting from a violation of this Act while the officer or employee was acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the State government;

(4) by an officer or employee of a government of a State that is not described in paragraph (3) may maintain a civil action for actual damages and for equitable relief against the officer or employee; or

(5) by an officer or employee of a government authority while the officer or employee was not acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the officer or employee.

(b) **KNOWING VIOLATIONS.**—Any individual entitled to recover actual damages under this section because of a knowing violation of a provision of this Act (other than subsection (c) or (d) of section 111) shall be entitled to recover the amount of the actual damages demonstrated or \$5000, whichever is greater.

(c) **ACTUAL DAMAGES.**—For purposes of this section, the term “actual damages” includes damages paid to compensate an individual for nonpecuniary losses such as physical and mental injury as well as damages paid to compensate for pecuniary losses.

(d) **PUNITIVE DAMAGES; ATTORNEY'S FEES.**—In any action brought under this section in which the complainant has prevailed because of a knowing violation of a provision of this Act (other than subsection (c) or (d) of section 111), the court may, in addition to any relief awarded under subsections (a) and (b), award such punitive damages as may be warranted. In such an action, the court, in its discretion, may allow the prevailing party a reasonable attorney's fee (including expert fees) as part of the costs, and the United States shall be liable for costs the same as a private person.

(e) **LIMITATION.**—A civil action under this section may not be commenced more than 2 years after the date on which the aggrieved individual discovered the violation or the date on which the aggrieved individual had a reasonable opportunity to discover the violation, whichever occurs first.

(f) **INSPECTION AND AMENDMENT.**—If a health information trustee has established a formal internal procedure that allows an individual who has been denied inspection or amendment of protected health information to appeal the denial, the individual may not maintain a civil action in connection with the denial until the earlier of—

(1) the date the appeal procedure has been exhausted; or

(2) the date that is 4 months after the date on which the appeal procedure was initiated.

(g) **NO LIABILITY FOR PERMISSIBLE DISCLOSURES.**—A health information trustee who makes a disclosure of protected health information about a protected individual that is permitted by this Act and not otherwise prohibited by State or Federal statute shall not be liable to the individual for the disclosure under common law.

(h) **NO LIABILITY FOR INSTITUTIONAL REVIEW BOARD DETERMINATIONS.**—If the members of a certified institutional review board have in good faith determined that an approved health research project is of sufficient importance so as to outweigh the intrusion into the privacy of an individual pursuant to section 116(a)(1), the members, the board, and the parent institution of the board shall not be liable to the individual as a result of such determination.

(i) **GOOD FAITH RELIANCE ON CERTIFICATION.**—A health information trustee who relies in good faith on a certification by a government authority or other person and discloses protected health information about an individual in accordance with this Act shall not be liable to the individual for such disclosure.

#### **SEC. 152. CIVIL MONEY PENALTIES.**

(a) **VIOLATION.**—Any health information trustee who the Secretary determines has demonstrated a pattern or practice of failure to comply with the provisions of this Act shall be subject, in addition to any other penalties that may be prescribed by law, to a civil money penalty of not more than \$10,000 for each such failure. In determining the amount of any penalty to be assessed under the procedures established under subsection (b), the Secretary shall take into account the previous record of compliance of the person being assessed with the applicable requirements of this Act and the gravity of the violation.

(b) **PROCEDURES FOR IMPOSITION OF PENALTIES.**—The provisions of section 1128A of the Social Security Act (other than subsections (a) and (b)) shall apply to the imposition of a civil monetary penalty under this section in the same manner as such provisions apply with respect to the imposition of a penalty under section 1128A of such Act.

#### **SEC. 153. ALTERNATIVE DISPUTE RESOLUTION.**

(a) **IN GENERAL.**—Not later than July 1, 1999, the Secretary shall, by regulation, develop alternative dispute resolution methods for use by individuals, health information trustees, and other persons in resolving claims under section 151.

(b) **EFFECT ON INITIATION OF CIVIL ACTIONS.**—

(1) **IN GENERAL.**—Subject to paragraph (2), the regulations established under subsection (a) may provide that an individual alleging that a right of the individual under this Act has been violated shall pursue at least one alternative dispute resolution method developed under such subsection as a condition precedent to commencing a civil action under section 151.

(2) **LIMITATION.**—Such regulations may not require an individual to refrain from commencing a civil action to pursue one or more alternative dispute resolution method for a period that is greater than 6 months.

(3) **SUSPENSION OF STATUTE OF LIMITATIONS.**—The regulations established by the Secretary under subsection (a) may provide that a period in which an individual described in paragraph (1) pursues (as defined by the Secretary) an alternative dispute resolution method under this section shall be excluded in computing the period of limitations under section 151(e).

(c) METHODS.—The methods under subsection (a) shall include at least the following:

- (1) ARBITRATION.—The use of arbitration.
- (2) MEDIATION.—The use of mediation.
- (3) EARLY OFFERS OF SETTLEMENT.—The use of a process under which parties make early offers of settlement.

(d) STANDARDS FOR ESTABLISHING METHODS.—In developing alternative dispute resolution methods under subsection (a), the Secretary shall ensure that the methods promote the resolution of claims in a manner that—

- (1) is affordable for the parties involved;
- (2) provides for timely and fair resolution of claims; and
- (3) provides for reasonably convenient access to dispute resolution for individuals.

**SEC. 154. AMENDMENTS TO CRIMINAL LAW.**

(a) IN GENERAL.—Title 18, United States Code, is amended by inserting after chapter 73 the following:

**“CHAPTER 74—OBTAINING PROTECTED HEALTH INFORMATION**

“Sec.

“1531. Definitions.

“1532. Obtaining protected health information under false pretenses.

“1533. Monetary gain from obtaining protected health information under false pretenses.

“1534. Knowing and unlawful obtaining of protected health information.

“1535. Monetary gain from knowing and unlawful obtaining of protected health information.

“1536. Knowing and unlawful use or disclosure of protected health information.

“1537. Monetary gain from knowing and unlawful sale, transfer, or use of protected health information.

**“§ 1531. Definitions**

“As used in this chapter—

“(1) the term ‘health information trustee’ has the meaning given such term in section 3(b)(5) of the Fair Health Information Practices Act of 1997;

“(2) the term ‘protected health information’ has the meaning given such term in section 3(a)(3) of such Act; and

“(3) the term ‘protected individual’ has the meaning given such term in section 3(a)(4) of such Act.

**“§ 1532. Obtaining protected health information under false pretenses**

“Whoever under false pretenses—

“(1) requests or obtains protected health information from a health information trustee; or

“(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee;

shall be fined under this title or imprisoned not more than 5 years, or both.

**“§ 1533. Monetary gain from obtaining protected health information under false pretenses**

“Whoever under false pretenses—

“(1) requests or obtains protected health information from a health information trustee with the intent to sell, transfer, or use such information for profit or monetary gain; or

“(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee with the intent to sell, transfer, or use such authorization for profit or monetary gain;

and knowingly sells, transfers, or uses such information or authorization for profit or monetary gain shall be fined under this title or imprisoned not more than 10 years, or both.

**“§ 1534. Knowing and unlawful obtaining of protected health information**

“Whoever knowingly obtains protected health information from a health information trustee in violation of the Fair Health Information Practices Act of 1997, knowing that such obtaining is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

**“§ 1535. Monetary gain from knowing and unlawful obtaining of protected health information**

“Whoever knowingly—

“(1) obtains protected health information from a health information trustee in violation of the Fair Health Information Practices Act of 1997, knowing that such obtaining is unlawful and with the intent to sell, transfer, or use such information for profit or monetary gain; and

“(2) knowingly sells, transfers, or uses such information for profit or monetary gain;

shall be fined under this title or imprisoned not more than 10 years, or both.

**“§ 1536. Knowing and unlawful use or disclosure of protected health information**

“Whoever knowingly uses or discloses protected health information in violation of the Fair Health Information Practices Act of 1997, knowing that such use or disclosure is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

**“§ 1537. Monetary gain from knowing and unlawful sale, transfer, or use of protected health information**

“Whoever knowingly sells, transfers, or uses protected health information in violation of the Fair Health Information Practices Act of 1997, knowing that such sale, transfer, or use is unlawful, shall be fined under this title or imprisoned not more than 10 years, or both.”

(b) CLERICAL AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 73 the following:

**“74. Obtaining protected health information ..... 1531”.**

**TITLE II—AMENDMENTS TO TITLE 5, UNITED STATES CODE**

**SEC. 201. AMENDMENTS TO TITLE 5, UNITED STATES CODE.**

(a) NEW SUBSECTION.—Section 552a of title 5, United States Code, is amended by adding at the end the following:

“(w) MEDICAL EXEMPTIONS.—The head of an agency that is a health information trustee (as defined in section 3(b)(5) of the Fair Health Information Practices Act of 1997) shall promulgate rules, in accordance with the requirements (including general notice) of subsections (b)(1), (b)(2), (b)(3), (c), and (e) of section 553 of this title, to exempt a system of records within the agency, to the extent that the system of records contains protected health information (as defined in section 3(a)(3) of such Act), from all provisions of this section except subsections (e)(1), (e)(2), subparagraphs (A) through (C) and (E) through (I) of subsection (e)(4), and subsections (e)(5), (e)(6), (e)(9), (e)(12), (l), (n), (o), (p), (q), (r), and (u).”

(b) REPEAL.—Section 552a(f)(3) of title 5, United States Code, is amended by striking “pertaining to him,” and all that follows through the semicolon and inserting “pertaining to the individual;”.

**TITLE III—REGULATIONS, RESEARCH, AND EDUCATION; EFFECTIVE DATES; APPLICABILITY; AND RELATIONSHIP TO OTHER LAWS**

**SEC. 301. REGULATIONS; RESEARCH AND EDUCATION.**

(a) REGULATIONS.—Not later than July 1, 1999, the Secretary shall prescribe regulations to carry out this Act.

(b) RESEARCH AND TECHNICAL SUPPORT.—The Secretary may sponsor—

(1) research relating to the privacy and security of protected health information;

(2) the development of consent forms governing disclosure of such information; and

(3) the development of technology to implement standards regarding such information.

(c) EDUCATION.—The Secretary shall establish education and awareness programs—

(1) to foster adequate security practices by health information trustees;

(2) to train personnel of health information trustees respecting the duties of such personnel with respect to protected health information; and

(3) to inform individuals and employers who purchase health care respecting their rights with respect to such information.

(d) OFFICE OF INFORMATION PRIVACY.—

(1) ESTABLISHMENT.—There is established in the Department of Health and Human Services, within the Office of the Secretary, an Office of Information Privacy. The Office of Information Privacy shall be headed by a Director, who shall also be the Privacy Adviser of the Department of Health and Human Services. The Director shall be the principal adviser to the Secretary on the effect of the use and disclosure of personally-identifiable information on the privacy of individuals.

(2) DUTIES.—The Director of the Office of Information Privacy shall—

(A) monitor and participate in the development of regulations under this Act;

(B) monitor the implementation of this Act within the Department of Health and Human Services;

(C) advise the Secretary of the effects of current activities and proposed statutory, regulatory, administrative, and budgetary actions on the information privacy of individuals;

(D) monitor the implementation within the Department of Health and Human Services of laws and policies affecting the confidentiality of personally-identifiable health information or other personally-identifiable information;

(E) advise the Secretary on the implications for privacy of automated systems for the collection, storage, analysis, or transfer of personally-identifiable health information or other personally-identifiable information;

(F) engage in, or commission, research and technical studies on the implications of policies and practices for information privacy promulgated by the Secretary;

(G) serve as a point of contact within the Department of Health and Human Services for persons, such as other agencies of the Federal Government, States, foreign governments, international organizations, privacy and consumer advocacy organizations, businesses, nonprofit organizations, and individuals, interested in the effects on privacy of the collection, maintenance, use, and disclosure of personally-identifiable health information or other personally-identifiable information; and

(H) report from time to time to the Secretary, the Congress, and the public on privacy matters.

**SEC. 302. EFFECTIVE DATES.**

(a) IN GENERAL.—Except as provided in subsection (b), this Act, and the amendments made by this Act, shall take effect on January 1, 2000.

(b) PROVISIONS EFFECTIVE IMMEDIATELY.—

(1) IN GENERAL.—A provision of this Act shall take effect on the date of the enactment of this Act if the provision—

(A) imposes a duty on the Secretary to develop, establish, or promulgate regulations, guidelines, notices, statements, or education and awareness programs; or

(B) authorizes the Secretary to sponsor research or the development of forms or technology.

(2) OFFICE OF INFORMATION PRIVACY.—Section 301(d) (relating to the Office of Information Privacy) shall take effect on the date of the enactment of this Act.

**SEC. 303. APPLICABILITY.**

(a) PROTECTED HEALTH INFORMATION.—Except as provided in subsections (b) and (c), the provisions of this Act shall apply to any protected health information that is received, created, used, maintained, or disclosed by a health information trustee in a State on or after January 1, 2000, regardless of whether the information existed or was disclosed prior to such date.

(b) EXCEPTION.—

(1) IN GENERAL.—The provisions of this Act shall not apply to a trustee described in paragraph (2), except with respect to protected health information that is received by the trustee on or after January 1, 2000.

(2) APPLICABILITY.—A trustee referred to in paragraph (1) is—

(A) a health researcher; or

(B) a person who, with respect to specific protected health information, received the information—

(i) pursuant to—

(I) section 117 (relating to emergency circumstances);

(II) section 118 (relating to judicial and administrative purposes);

(III) section 119 (relating to law enforcement); or

(IV) section 120 (relating to subpoenas, warrants, and search warrants); or

(ii) while acting in whole or in part in the capacity of an officer or employee of a person described in clause (i).

(c) **AUTHORIZATIONS FOR DISCLOSURES.**—An authorization for the disclosure of protected health information about a protected individual that is executed by the individual before January 1, 2000, and is recognized and valid under State law on December 31, 1999, shall remain valid and shall not be subject to the requirements of section 112 until January 1, 2001, or the occurrence of the date or event (if any) specified in the authorization upon which the authorization expires, whichever occurs earlier.

**SEC. 304. RELATIONSHIP TO OTHER LAWS.**

(a) **STATE LAW.**—Except as otherwise provided in subsections (b), (c), (d), (e), and (g), a State may not establish, continue in effect, or enforce any State law to the extent that the law is inconsistent with, or imposes additional requirements with respect to, any of the following:

(1) A duty of a health information trustee under this Act.

(2) An authority of a health information trustee under this Act to disclose protected health information.

(3) A provision of subtitle C (relating to access procedures and challenge rights), subtitle D (miscellaneous provisions), or subtitle E (relating to enforcement).

(b) **LAWS RELATING TO PUBLIC HEALTH AND MENTAL HEALTH.**—This Act does not preempt, supersede, or modify the operation of any State law regarding public health or mental health to the extent that the law prohibits or regulates a disclosure of protected health information that is permitted under this Act.

(c) **CRIMINAL PENALTIES.**—A State may establish and enforce criminal penalties with respect to a failure to comply with a provision of this Act.

(d) **REQUIREMENTS ON STATE AGENCIES.**—A State may establish, continue in effect, and enforce any State law to the extent that the law imposes on a judicial, legislative, or executive agency of the State a requirement, limitation, or procedure with respect to the use or disclosure of protected health information that is in addition to the requirements, limitations, and procedures imposed under this Act.

(e) **PRIVILEGES.**—A privilege that a person has under law in a court of a State or the United States or under the rules of any agency of a State or the United States may not be diminished, waived, or otherwise affected by—

(1) the execution by a protected individual of an authorization for disclosure of protected health information under this Act, if the authorization is executed for the purpose of receiving health care or providing for the payment for health care; or

(2) any provision of this Act that authorizes the disclosure of protected health information for the purpose of receiving health care or providing for the payment for health care.

(f) **DEPARTMENT OF VETERANS AFFAIRS.**—The limitations on use and disclosure of protected health information under this Act shall not be construed to prevent any exchange of such information within and among components of the Department of Veterans Affairs that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

(g) **CERTAIN DUTIES UNDER STATE OR FEDERAL LAW.**—This Act shall not be construed to preempt, supersede, or modify the operation of any of the following:

(1) Any law that provides for the reporting of vital statistics such as birth or death information.

(2) Any law requiring the reporting of abuse or neglect information about any individual.

(3) Subpart II of part E of title XXVI of the Public Health Service Act (relating to notifications of emergency response employees of possible exposure to infectious diseases).

(4) The Americans with Disabilities Act of 1990.

(5) Any Federal or State statute that establishes a privilege for records used in health professional peer review activities.

(h) **SECRETARIAL AUTHORITY.**—

(1) **SECRETARY OF HEALTH AND HUMAN SERVICES.**—A provision of this Act does not preempt, supersede, or modify the operation of section 543 of the Public Health Service Act, except to the extent that the Secretary of Health and

Human Services determines through regulations promulgated by such Secretary that the provision provides greater protection for protected health information, and the rights of protected individuals, than is provided under such section 543.

(2) SECRETARY OF VETERANS AFFAIRS.—A provision of this Act does not preempt, supersede, or modify the operation of section 7332 of title 38, United States Code, except to the extent that the Secretary of Veterans Affairs determines through regulations promulgated by such Secretary that the provision provides greater protection for protected health information, and the rights of protected individuals, than is provided under such section 7332.

Mr. HORN. No one will make the mistake of thinking that medical privacy is a new issue. It is worth recalling the words of Hippocrates. His oath included the following pledge: "All that may come to my knowledge in the exercise of my profession, which ought not to be spread abroad, I will keep secret and will never reveal."

Patient information acquired by medical experts is deeply personal and should be kept private. The challenge we now face is to protect the timeless value of confidentiality, the privacy between doctor and patient, in a rapidly changing health care environment. We face an enormous conflict between an old value, the right to personal privacy, and the increasing need of our health care system to exchange intimate information about each of us. Managed health care systems must be able to exchange information between doctors, insurers, and others. We need to set the rules of the road.

At stake are the quality and the value of our health care. The increasing use of information technology and the increasing complexity of provider arrangements are inevitable. The exchange of patient health care information is an integral part of the existing health care system. Claims payments require diagnostic information. Communications between primary care providers and other providers, such as specialists or hospitals, require patient information to be shared. Pharmacies maintain data bases of past prescriptions.

Despite this highly fluid environment for exchanging health care information, no uniform national standard currently exists to protect the confidentiality of this information. Moreover, there is little uniformity among State statutes regarding the confidentiality of health care information. Most of the States' laws lack penalties for misuse or misappropriation. Protections vary according to both the holder and the type of information.

Under last year's Kassebaum-Kennedy act, the Secretary of Health and Human Services is required to recommend privacy standards for health care information to Congress by September 1997. If Congress does not enact health care privacy legislation by August 1999, the Secretary of Health and Human Services is required to promulgate such privacy regulations. In effect, the Kassebaum-Kennedy act gave Congress a 3-year window of opportunity to enact major health care privacy legislation.

An illustration of the difficulties we face is the revolution in the science of genetics, with the mapping of the human genome. Incredibly sensitive, precise genetic tests have been developed, genetic screening has become commonplace, and an extraordinary array of genetic interventions are being explored.

Genetics privacy issues inevitably accompany the scientific advances. Do genetic data differ fundamentally from other health

data? Genetic data could be used prejudicially, such as ineligibility for employment, financial credit, or life or health insurance.

Issues associated with genetic privacy and possible discrimination based on genetic information have received heightened attention. The House Committee on Commerce has established a task force on health records and genetic privacy chaired by Representative Stearns and Green. Any substantial legislation on the issue of medical records privacy will involve establishing uniform national rules on the collection and protection of personally identifiable health data, affirming the rights of patients, setting criteria and procedures for disclosure, their use and security of health care information, focusing responsibilities for ensuring proper protection and use of health care information and establishing penalties for wrongful use of the data.

The legislation before us today is H.R. 52, the Fair Health Information Practices Act of 1997. Under this bill, medical records created or used during the process of treatment become protected health information. Furthermore, health care providers are required to maintain appropriate administrative, technical, and physical safeguards to protect the integrity and privacy of health care information. H.R. 52 would allow patients to review their medical records and correct inaccurate information. It would also place restriction on the release of information relating to the treatment of patients and on the payment for health care services.

Three Members of Congress who have taken the lead on medical records privacy issues will testify today as part of our first panel. They are Representative Condit, who is author of H.R. 52, as well as Representatives Slaughter and Stearns.

Representatives of privacy advocates, health care providers and records management organizations will testify on panel II. The witnesses are Ms. Janlori Goldman, visiting scholar at Georgetown University Law Center, who is also affiliated with the Center for Democracy and Technology; Dr. Donald J. Palmisano, who is a member of the Board of Trustees, American Medical Association; and Dr. Merida Johns, who is president of the American Health Information Management Association.

Representatives of medical researchers will testify on panel III. Witnesses are Dr. Sherine Gabriel of the Department of Health Services Research, Mayo Clinic, representing the Health Care Leadership Council; Dr. Elizabeth Andrews of Glaxo Wellcome, representing the Pharmaceutical Research and Manufacturers Association; and Dr. Steven Kenny Hoge, who serves as chair of the Council on Psychiatry and Law at the American Psychiatric Association.

We welcome all of today's witnesses.

I have just learned that Mrs. Slaughter will not be here. She asks for her comments to be submitted for the record and without objection, they will be. We are delighted to have the author of this legislation with us, Mr. Condit, and it is all yours.

**STATEMENT OF HON. GARY A. CONDIT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA**

Mr. CONDIT. Thank you, Mr. Chairman. First of all, let me commend you, Mr. Chairman, for gathering us here today to discuss

the privacy of medical records. This is an extremely important step in addressing the anxiety of many patients and citizens across this country. The time has come for us in reforming the way we handle medical records; and this is a very sensitive issue, and it is time for us to take a look at how we have been doing this.

As more and more medical records are computerized, a patient's confidentiality is put at risk, and we have examples of that throughout our review of this issue. For this reason, I have introduced the Fair Health Information Practices Act; and you have been kind enough to work with us on that, Mr. Chairman and I appreciate that very much.

Our guiding principle in drafting this bill is to protect the confidential information contained in medical records and protecting this information once it leaves the physician's office. Under the bill, medical information is protected by establishing uniform Federal rules for handling medical records; holding those who handle this information accountable for the security and privacy of the medical records.

Today, you will hear testimony from a number of people who have expertise in this area, and I look forward to their testimony. We have heard them speak before, over the last couple of years, on this issue. You know, last year, with the Kennedy-Kassebaum bill, we were given a target date, 1999, to enact something. We think this is a good step in the right direction, and I hope we can put something together.

Mr. Chairman, I have an extensive statement and some background information that I would like to submit for the record, and I would be available here for a few minutes to respond to any comments or questions; and with that, I will yield back.

Mr. HORN. Well, we appreciate you coming and your statement will be, without objection, part of the record at this point.

Mr. CONDIT. Thank you.

[The prepared statement of Hon. Gary A. Condit follows:]

**Statement of Representative Gary A. Condit  
June 5, 1997**

I want to thank the Subcommittee for holding this hearing on health information privacy. It is important to begin the legislative process now. Last year's Kennedy-Kassebaum law (Health Insurance Portability and Accountability Act of 1996) established a three year deadline for legislative action. That deadline falls in August 1999, in the middle of the first session of the next Congress (the 106th). It is unlikely, however, that a major piece of legislation like a health privacy law will make it through so quickly in the first session of a new Congress. This means, as a practical matter, that we should work toward the goal of passing a bill by the end of this Congress in the fall of 1998.

Several recent studies document the need for uniform federal health confidentiality legislation. The Office of Technology Assessment, the Institute of Medicine, and this Committee during the 103rd Congress all found that the present system of protecting health care information is based on a patchwork quilt of laws. The simple truth is that health information has little meaningful legal protection today. A new report issued this year by the Computer Science and Telecommunications Board of the National Research Council reached the same conclusion.

In the 103rd Congress, I proposed the Fair Health Information Practices Act. This represented the first comprehensive attempt to address health privacy through federal legislation since 1980. My bill passed the Government Operations Committee in 1994, but it died with the rest of health reform. I reintroduced the bill in the last Congress as H.R. 435. This year, the bill is H.R. 52. An explanation of the changes that I made to this year's bill appears at the end of this statement.

The purpose of my legislation is to establish a uniform federal code of fair information practices for individually identifiable health information in the health treatment and payment process. More information about the background and the substance of my proposal can be found in House Report 103-601 Part 5. The report contains a detailed discussion of how to address health privacy in federal legislation.

My legislation is not a pie-in-the sky privacy code. It is a realistic bill for the real world. We have to recognize that we cannot elevate each patient's privacy interest above every other societal interest. That would be impractical, unrealistic, and expensive. The right answer is to strike an appropriate balance that protects each patient's interests while permitting essential uses of data under controlled conditions. That is what H.R. 52 does.

One goal of my bill is to change the culture of health records so that professionals and patients alike will be able to understand the rights and responsibilities of all participants. Common rules will facilitate broader understanding and better protection. Professionals will be able to learn the rules with the confidence that the same rules will apply wherever they practice. Patients will learn that they have the same rights in every state and in every doctor's office.

Under H.R. 52, there will be no loopholes for protected health information. As

data moves through the health care system and beyond, it will remain subject to a common set of rules. This may be the single most important feature of the bill.

There are limits, however, to what can be accomplished through legislation. The health care system is tremendously complex, and much of the treatment, payment, and oversight activity is necessarily fueled by identifiable data. Legislation passed in recent years has greatly contributed to the increased use of patient data to limit costs, combat fraud, and improve care. Those remain important goals along with protecting privacy.

Still, we need to minimize the use of identifiable data, and this is one of several areas where my bill needs more work. The use of coded and encrypted data can be expanded in a way that satisfies the needs of data users and still fully protects the privacy interests of patients. I don't think that we can expect to solve all of the problems by removing identifiers all of the time, but we can do better. Increased computerization of health records presents new challenges to protecting patient privacy, but this is one area where computers can help to increase protections by allowing the cost-effective creation and manipulation of useful but non-identifiable information.

It would be wonderful if we could restore the old notion that what you tell your doctor in confidence remains totally secret. In a health care environment, characterized by third party payers, medical specialization, high-cost care, and increasing computerization, absolute privacy is simply not possible. What is possible is to assure people that information will be used in accordance with a code of fair information practices.

The promise of that code to professionals and patients alike is that identifiable health information will be fairly treated. There will be a clear set of rules that protect the confidentiality interests of each patient to the greatest extent possible. While we may not realistically be able to offer any more than this, we surely can do no less.

There were several other health privacy bills in both the House and the Senate last year. Each of the bills offered something new and useful. More proposals will surely emerge as the Congress progresses. There is broad agreement on the general goals of legislation, but little consensus on the details.

What is needed now is for this Subcommittee to begin working on those details. Many of the differences that exist can be resolved through hard work and better understanding. We need to settle as many technical problems as we can before moving on to the difficult policy questions that will surely remain. I am prepared to work with this Subcommittee and with others to move the process forward as quickly as possible.

#### Changes in H.R. 52 From Earlier Versions

H.R. 52 is largely similar to H.R. 435, but I made several changes based on new ideas and developments that emerged in the last two years. The substantive changes in this year's proposal are:

- 1) References to "health information service organizations" have been dropped.

This was a place holder for other institutions that were being developed in the context of broad health care reform. The references are no longer meaningful.

2) The section on "Accounting for Disclosures" has been retitled as "Disclosure History." Nothing substantive was changed, but the new language is more descriptive.

3) In section 101, I added language to the patient access section making it clear that copies of records have to be provided to the patient in any form or format requested by the patient if the record is readily reproducible by the trustee in that form or format. The language was inspired in part by the recently passed Electronic Freedom of Information Amendments. The purpose is to make sure that a patient can have a record in a format that will be meaningful to the patient or useful to other health care providers.

4) Also in section 101, the exception to patient access for mental health treatment notes has been eliminated. The policy of the bill is that a patient should have broad access to his or her health record. Exceptions are provided only when there is a direct conflict with another interest or when access is meaningless or pointless. The only substantive exception had been for mental health treatment notes. Given the broad sweep of the access provision, I am not sure that this exception can be justified any more. I left it out this year so that the advocates of the exception would have to come forward to argue for its inclusion and make their case on the public record. I could be persuaded to reinstate the mental health treatment note exception if it can be justified. The burden should be on the proponents of the exception.

5) New language in section 301(d) creates an Office of Information Privacy in the Department of Health and Human Services. The head of the office is the Privacy Advisor to the Department. This is not really a new office. The Department recently established a Privacy Advocate. The purpose of the new legislative language is to define the health privacy functions of this office with more precision and permanence.

6) Section 304 of the bill deals with preemption of state laws. This is a difficult subject that clearly need more work and more thought. I added one new idea this year. New language provides that the states may impose additional requirements on its own agencies with respect to the use or disclosure of protected health information. The idea is a simple one. If a state wants to impose more stringent restrictions on the ability of state police, state fraud investigators, or other state offices to use or disclose protected health information, it may do so.

In this instance, higher standards will not interfere with access to or use of information by other authorized users or by the federal government. The goal is to allow states to set as high a floor as they choose with respect to their own activities. This will not undermine the uniformity principle otherwise reflected in the bill, and it will not affect the drive for administrative simplification or uniform technical standards. Only state agencies will be affected by my new language. I thought that this idea was worth including so that it would attract comment. The language itself may need further tweaking. The issue of uniformity and preemption will be difficult and contentious, and I wanted to add this new idea to the discussion.

Mr. HORN. We now have the distinguished Member from Florida, Mr. Stearns.

**STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA**

Mr. STEARNS. Good morning, Mr. Chairman. I am delighted to be here and want to compliment you on your leadership in having this hearing. While the scope of your hearing today covers medical records in general, I would like to restrict my comments to why I believe we must provide safeguards to prevent discrimination based on a person's genetic profile.

The question of confidentiality of one's medical record is something that should concern us all. The reason I am here today is to discuss how we can find a way to ensure that technological advances in genetic testing proceed while protecting the interests of the individual.

Let me state, technology is good, research must be allowed. It is the means and applications of this technology and research that concerns us all. I believe genetic testing may become, in fact, a civil rights issue. It could be the civil rights issue of the 21st century. Should an insurance company be able to deny children medical coverage because their mother died of an inherited heart defect? Even if children may or may not carry the defect this is a dilemma faced by a father in California who could not get family medical coverage under his group plan as a result of his wife's death.

In another case, a man lost his auto insurance coverage because he had a genetic condition which affected his muscles. Although he had a clean driving record stretching back 20 years, genetic information was used to cancel his policy.

One young woman was hired as a social worker, and for 8 months, she received promotions and positive performance reviews. However, while conducting a training program on caring for patients with Huntington's disease, she mentioned that she had family members with that condition. She was soon fired and informed by another colleague that it was due to a concern that she might develop Huntington's disease.

As these cases show, access to genetic information can result in being denied health insurance, cancellation of auto insurance, and even the loss of a job. These people were discriminated against based upon their genes. You might be amazed to know how many of us here in this committee room carry mutated genes. The fact is, we all do. Fortunately, most genetic mutations are silent, exhibiting no significant consequences.

The National Institutes for Health is home to the Human Genome Project. This project is a 15-year study scheduled for completion in the year 2005. The discoveries made from mapping out the entire human genome will mean better early detection, treatment of disease, and even their prevention. These are the up sides of genetic research.

The examples I provided earlier show genetic information can also be used to discriminate against people. That is where Congress should take action to ensure continued progress in genetic research while also protecting people from the misuse of genetic information.

This issue is moving very quickly, and we need to make some sound public policy decisions now.

In the last Congress, I introduced the Genetic Privacy and Non-discrimination Act, H.R. 2690, to establish guidelines concerning the disclosure and use of genetic information. My goal was to protect the health privacy of the American people while not disrupting genetic research efforts. I am currently drafting a similar piece of legislation for the 105th Congress.

Last year, I was able to, with the help of others, insert language into the Health Care Coverage and Affordability Act while the measure was in the Commerce Committee, on which I sit. As you know, we passed this measure and the President signed it. One provision of this bill prohibits insurance companies from denying coverage to an employee or beneficiary on the basis of health status. Health status was defined as an individual's medical condition, claims, experience, receipt of health care, medical history, evidence of insurability, or disability. The two words that I inserted in the commerce bill were, quote, genetic information. These two words made a good bill better, but additional protection and guidelines are still needed. That is one of my priorities in the 105th Congress.

Chairman Tom Bliley of the Commerce Committee asked me to take a leading role in establishing policy on these issues by chairing the task force on health records and genetic privacy. This bipartisan task force will consider these questions in a series of briefings, meetings, and public hearings.

The job of the task force is to answer a number of questions which certainly pertain to medical records and privacy; and some of these are, Mr. Chairman, one, how will we protect the health records of persons with genetic deficiencies and still allow scientific research to go forward unimpeded? Additionally, the whole area of, quote, informed consent, end quote, must be clarified as it pertains to genetic privacy. How will the thousands of available genetic tests created as a result of the Human Genome Project affect our citizens? And three, what issues are raised by the potential misuse of genetic and other information about an individual?

Genetic information is personal, powerful, permanent, and sensitive. It not only affects the individual, but it also has an impact on offspring and other blood relatives. Genetic privacy must be protected. On the other hand, it is a key to the treatment, cure and prevention of disease, so genetic research must continue. I see our job is to meet these goals as best we can; it is also an issue of fairness.

In conclusion, Mr. Chairman, think about those two little boys in California who were denied insurance coverage because of an error in a genetic script. This is something that they could not control and did not choose. As I noted, we all have errors in our genetic blueprints. For most of us, it does not harm us, but for many, the onset of disease is devastating. We owe them a level of privacy and the hope for treatment and cure. That is the central mission of my task force and legislation.

Thank you, Mr. Chairman.

Mr. HORN. I thank you for that very fine statement.

[The prepared statement of Hon. Cliff Stearns follows:]

STATEMENT OF THE HONORABLE CLIFF STEARNS  
ON MEDICAL RECORDS PRIVACY: H.R. 52  
BEFORE THE  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION AND TECHNOLOGY  
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT  
JUNE 5, 1997

GOOD MORNING. I WANT TO THANK YOU CHAIRMAN HORN FOR INVITING ME TO TESTIFY BEFORE YOUR SUBCOMMITTEE TODAY ON MEDICAL RECORDS PRIVACY.

WHILE THE SCOPE OF YOUR HEARING TODAY COVERS MEDICAL RECORDS IN GENERAL, I WOULD LIKE TO RESTRICT MY COMMENTS TO WHY I BELIEVE WE MUST PROVIDE SAFEGUARDS TO PREVENT DISCRIMINATION BASED UPON A PERSON'S GENETIC PROFILE.

THE QUESTION OF CONFIDENTIALITY OF ONE'S MEDICAL RECORDS IS SOMETHING THAT SHOULD CONCERN US ALL. THE REASON I AM HERE TODAY IS TO DISCUSS HOW WE CAN FIND A WAY TO ENSURE THAT TECHNOLOGICAL ADVANCES IN GENETIC TESTING PROCEED WHILE PROTECTING THE INTERESTS OF THE INDIVIDUAL. LET ME STATE THAT TECHNOLOGY IS GOOD, IT IS THE MEANS OF ITS APPLICATION THAT MUST CONCERN US.

I BELIEVE THAT GENETIC TESTING MAY BECOME THE CIVIL RIGHTS ISSUE OF THE 21ST CENTURY. SHOULD AN INSURANCE COMPANY BE ABLE TO DENY CHILDREN

MEDICAL COVERAGE BECAUSE THEIR MOTHER DIED OF AN INHERITED HEART DEFECT THAT HER CHILDREN MAY OR MAY NOT CARRY? THAT IS THE DILEMMA FACED BY A FATHER IN CALIFORNIA WHO COULD NOT GET FAMILY MEDICAL COVERAGE UNDER HIS GROUP PLAN AS A RESULT OF HIS WIFE'S DEATH.

IN ANOTHER INSTANCE, A MAN LOST HIS AUTO INSURANCE COVERAGE BECAUSE HE HAD A GENETIC CONDITION WHICH AFFECTS THE MUSCLES. ALTHOUGH HE HAD A CLEAN DRIVING RECORD STRETCHING BACK 20 YEARS, GENETIC INFORMATION WAS USED TO CANCEL HIS POLICY.

ONE YOUNG WOMAN WAS HIRED AS A SOCIAL WORKER AND FOR EIGHT MONTHS SHE RECEIVED PROMOTIONS AND POSITIVE PERFORMANCE REVIEWS. HOWEVER, WHILE CONDUCTING A TRAINING PROGRAM ON CARING FOR PATIENTS WITH HUNTINGTON'S DISEASE, SHE MENTIONED THAT SHE HAD FAMILY MEMBERS WITH THAT CONDITION. SHE WAS SOON FIRED AND INFORMED BY ANOTHER COLLEAGUE THAT IT WAS DUE TO CONCERN THAT SHE MIGHT DEVELOP HUNTINGTON'S.

AS THESE CASES SHOW, ACCESS TO GENETIC INFORMATION CAN RESULT IN BEING DENIED HEALTH INSURANCE, CANCELLATION OF AUTO INSURANCE, AND

EVEN THE LOSS OF A JOB. THESE PEOPLE WERE DISCRIMINATED AGAINST BASED UPON THEIR GENES.

YOU MIGHT BE AMAZED TO KNOW HOW MANY OF US HERE IN THIS COMMITTEE ROOM CARRY MUTATED GENES. THE FACT IS -- WE ALL DO. FORTUNATELY, MOST GENETIC MUTATIONS ARE "SILENT," EXHIBITING NO SIGNIFICANT CONSEQUENCES.

THE NIH IS HOME TO THE HUMAN GENOME PROJECT. THIS PROJECT IS A 15-YEAR STUDY WHICH IS SCHEDULED FOR COMPLETION IN 2005. THE DISCOVERIES MADE FROM MAPPING OUT THE ENTIRE HUMAN GENOME WILL MEAN BETTER EARLY DETECTION, TREATMENT OF DISEASE, AND EVEN THEIR PREVENTION.

THESE ARE THE UPSIDES OF GENETIC RESEARCH. AS THE EXAMPLES I PROVIDED EARLIER SHOW, GENETIC INFORMATION CAN ALSO BE USED TO DISCRIMINATE AGAINST INDIVIDUALS. THAT IS WHERE CONGRESS MUST TAKE ACTION -- TO ENSURE CONTINUED PROGRESS IN GENETIC RESEARCH WHILE ALSO PROTECTING PEOPLE FROM THE MISUSE OF GENETIC INFORMATION. THIS ISSUE IS MOVING QUICKLY AND WE NEED TO MAKE SOME SOUND PUBLIC-POLICY DECISIONS NOW.

IN THE LAST CONGRESS I INTRODUCED THE GENETIC PRIVACY AND NONDISCRIMINATION ACT (H.R. 2690), TO ESTABLISH GUIDELINES CONCERNING THE DISCLOSURE AND USE OF GENETIC INFORMATION. MY GOAL WAS TO PROTECT THE HEALTH PRIVACY OF THE AMERICAN PEOPLE WHILE NOT DISRUPTING GENETIC RESEARCH EFFORTS. I AM CURRENTLY DRAFTING SIMILAR LEGISLATION FOR THE 105TH CONGRESS.

LAST YEAR I WAS ALSO ABLE TO INSERT LANGUAGE INTO THE HEALTH COVERAGE AND AFFORDABILITY ACT WHILE THE MEASURE WAS IN THE COMMERCE COMMITTEE, ON WHICH I SIT. AS YOU KNOW, WE PASSED THIS MEASURE AND THE PRESIDENT SIGNED IT. ONE PROVISION OF THIS BILL PROHIBITS INSURANCE COMPANIES FROM DENYING COVERAGE TO AN EMPLOYEE OR BENEFICIARY ON THE BASIS OF "HEALTH STATUS." HEALTH STATUS WAS DEFINED AS AN INDIVIDUAL'S "MEDICAL CONDITION, CLAIMS EXPERIENCE, RECEIPT OF HEALTH CARE, MEDICAL HISTORY, EVIDENCE OF INSURABILITY, OR DISABILITY."

THE TWO WORDS I INSERTED WERE ADDED TO THIS LIST -- THEY WERE "GENETIC INFORMATION." THESE TWO WORDS MADE A GOOD BILL BETTER. BUT ADDITIONAL PROTECTION AND GUIDELINES ARE NEEDED. THAT IS ONE OF MY TOP PRIORITIES FOR THE 105TH CONGRESS.

CHAIRMAN TOM BLILEY ASKED ME TO TAKE A LEADING ROLE IN ESTABLISHING POLICIES ON THESE ISSUES BY CHAIRING THE TASK FORCE ON HEALTH RECORDS AND GENETIC PRIVACY. THIS BIPARTISAN TASK FORCE WILL CONSIDER THESE QUESTIONS IN A SERIES OF BRIEFINGS, MEETINGS, AND PUBLIC HEARINGS.

THE JOB OF THE TASK FORCE IS TO ANSWER A NUMBER OF QUESTIONS WHICH CERTAINLY PERTAIN TO MEDICAL RECORDS AND PRIVACY. SOME OF THESE INCLUDE--

- HOW WILL WE PROTECT THE HEALTH RECORDS OF PERSONS WITH GENETIC DEFICIENCIES AND STILL ALLOW SCIENTIFIC RESEARCH TO GO FORWARD UNIMPEDED. ADDITIONALLY, THE WHOLE AREA OF "INFORMED CONSENT" MUST BE CLARIFIED AS IT PERTAINS TO GENETIC PRIVACY.
- HOW WILL THE THOUSANDS OF AVAILABLE GENETIC TESTS CREATED AS A RESULT OF THE HUMAN GENOME PROJECT AFFECT OUR CITIZENS? AND,
- WHAT ISSUES ARE RAISED BY THE POTENTIAL MISUSE OF GENETIC AND OTHER INFORMATION ABOUT AN INDIVIDUAL?

GENETIC INFORMATION IS PERSONAL, POWERFUL, PERMANENT, AND SENSITIVE. IT NOT ONLY AFFECTS THE INDIVIDUAL, BUT IT ALSO HAS AN IMPACT ON OFFSPRING AND OTHER BLOOD RELATIVES. GENETIC PRIVACY MUST BE PROTECTED. ON THE OTHER HAND, GENETIC RESEARCH IS THE KEY TO THE TREATMENT, CURE, AND PREVENTION OF DISEASE. GENETIC RESEARCH MUST BE CONTINUED.

I SEE OUR JOB IS TO MEET THESE GOALS AS BEST AS WE CAN. IT IS ALSO AN ISSUE OF FAIRNESS. THINK ABOUT THOSE TWO LITTLE BOYS IN CALIFORNIA WHO WERE DENIED INSURANCE COVERAGE BECAUSE OF AN ERROR IN A GENETIC SCRIPT THAT THEY COULD NOT CONTROL AND DID NOT CHOOSE. AS I NOTED, WE ALL HAVE ERRORS IN OUR GENETIC BLUEPRINT. FOR MOST OF US IT DOES NO HARM -- BUT FOR MANY THE ONSET OF DISEASE IS DEVASTATING. WE OWE THEM A LEVEL OF PRIVACY AND THE HOPE FOR TREATMENT AND CURES. THAT IS THE CENTRAL MISSION OF MY TASK FORCE AND OF MY LEGISLATION.

THANK YOU VERY MUCH.

Mr. HORN. Let me just put in the record, without objection, the comments of Representative Shays, who is chairman of the Human Resources Subcommittee of our full committee and the comments of Representative Slaughter, who is the author of H.R. 306, the Genetic Information Nondiscrimination and Health Insurance Act. Any other remarks as Members arrive, those opening statements will be put in the record.

[The prepared statements of Hon. Christopher Shays and Hon. Louise M. Slaughter follow:]

**Statement of Congressman Christopher Shays**  
Before the Subcommittee on Government Management, Information and  
Technology of the Committee on Government Reform and Oversight  
*June 5, 1997*

Thank you Mr. Chairman and Members of the Subcommittee for the opportunity to provide you with my thoughts on medical records confidentiality.

With the dramatic increase in technology, the dissemination of information and the development of coordinated care systems in which data is regularly shared by a number of individuals, the need for protecting consumers' medical records is essential. Improper disclosure of sensitive medical records can damage careers, reputations and relationships.

At the same time, insurers, providers, managed care networks and law enforcement need to access information to pay claims and provide exceptional care and detect fraud and abuse. In addition, researchers need medical data to improve the effectiveness and efficiency of health practices and advance scientific knowledge.

Unfortunately, as we've discovered, there is a patchwork of state initiatives and some federal law that protects some patients but not others, and very often unequally. As Daniel Mendelson and Eileen Miller Salinsky point out in the May/June 1997 issue of *Health Affairs*:

*Confidentiality of personal records and security of data systems have long been recognized as critical. States need to set levels of access to different types of data, ensure that data systems are secure, and protect patient confidentiality. Although these objectives are universally articulated by states, interpretations vary, and many basic questions (such as ownership of patient records) remain unresolved.*

A uniform standard that applies evenly across state lines should be developed that empowers the individual to control the use of personal health information irrespective of state law. In short, federal standards are necessary.

In addition, the prevalence of managed care networks and the delivery of coordinated care has increased access to high quality, low cost care. Managed care networks evolved in the late 1980s and early 1990s as a response to the spiraling health care costs that were crippling the ability of businesses and individuals to maintain affordable health insurance coverage. In response, managed care provided

an alternative and allowed many families an option in how they receive care. We should be careful not to hinder the ability of managed care plans to continue this coverage when developing federal standards for protecting medical records.

I am glad the Health Insurance Portability and Accountability Act (HIPPA) took a step in the right direction in simplifying administrative procedures. A part of the administrative simplification provision called upon the Health and Human Services (HHS) Secretary to report to Congress detailed recommendations on standards with respect to individually identifiable health information. Should Congress fail to act, HHS will implement regulations to ensure confidentiality.

We need to finish the job of protecting consumers by ensuring Congress, not HHS, implements standards of confidentiality for medical records.

Mr. Chairman, I am glad you have taken this step to begin discussion on this critical issue. I look forward to working with you and other Members of Congress to craft a proposal that protects consumers while ensuring high quality care. I especially appreciate the good work of Senator Bennett and his staff on this important issue. As I have discovered, drafting an even handed bill that protects consumers while ensuring the continuity of care is a difficult task.

Increasingly we hear news accounts of individuals accessing confidential medical information. Just last month, a Reuters article reported that a funeral director in Florida sent to two newspapers a list of almost 4,000 HIV-positive patients he obtained from the laptop computer that his live-in companion, a state health worker, brought home from work. According to the news account, "Neither newspaper published the list, but panic ensued among patients who feared publicity could cost them friends, jobs and insurance coverage." Reuters reported the incident was the nation's largest security breach of confidential information about HIV-positive individuals, and that the man could face up to 60 days in jail.

With current technology and future technological advances there are both real dangers and substantial opportunities with respect to protected health information. Absent strong, practical and workable protections, many will fall victim to those dangers and opportunities missed. It is my hope Members of both parties can work together to craft a sensible bill that capitalizes on the opportunities presented by new technologies.

Mr. Chairman, I appreciate the opportunity to testify and am happy to answer any questions you may have.

**Testimony of Rep. Louise Slaughter  
before the Government Reform Subcommittee on Government Management, Information,  
and Technology  
Hearing on Medical Records Privacy**

June 5, 1997

Mr. Chairman, I am grateful for the opportunity to testify before the Subcommittee on Government Management, Information, and Technology on medical records privacy today. I commend you for your leadership on this most important issue, which is of great concern to so many Americans.

As you know, I am the sponsor of H.R. 306, the Genetic Information Nondiscrimination in Health Insurance Act. I am proud to count you, Chairman Horn, as well as subcommittee members Reps. Maloney, Owens, and Davis among the bill's 123 cosponsors. This legislation would prevent health insurance companies from discriminating against consumers based on their genetic information. In addition, it contains a strong medical records privacy component. Insurers are prohibited from requesting or requiring that an individual disclose genetic information as a condition of coverage. Further, my bill would require prior, written, informed consent before genetic information could be revealed to any third party.

Mr. Chairman, Americans are growing increasingly concerned about the privacy -- or vulnerability -- of their medical records. While many people believe their medical records are closed to everyone except their health care provider and insurer, the truth is very different. On February 4, a *New York Times* article recounted how one doctor started investigating how many people had access to his patients' records after being confronted with one patient's fear of disclosure. He said, and I quote, "I stopped counting at 75." This incident happened a decade ago. The situation is even more extreme today.

Doctors, nurses, therapists, and secretaries are only a few of the people who have access to an individual's medical charts. Today our medical records may also be viewed by consultants, billing clerks, insurance "coders," and many others. An employer may have free access to workers' records, especially if the company is self-insured. Medicare sees the records of elderly and disabled patients, while Medicaid workers may view medical charts for the poor. The potential for genetic discrimination and other misuse of this information is staggering.

The computerization of medical records has exacerbated this situation. Many insurers pool medical information in the Medical Information Bureau, which may distribute it to any number of sources. Marketers buy sophisticated lists of health and demographic information to help them target their products. Lawyers look at records in the context of rape, domestic violence, and medical injury cases. Equifax and other credit reporting services can get access. The list goes on and on.

The computerization of medical records has added a new urgency to the need for regulations to protect consumers. In the past, the practical limitations of paper records made access more difficult. Computerization of records means that large numbers of medical records can be screened, collated, and distributed in the blink of an eye. Information can be made available to almost unlimited numbers of people via the Internet. The market for medical records information is booming, and there is reputed to be a vigorous black market for it as well.

My legislation would provide comprehensive protection for all Americans against genetic discrimination in health insurance. The bill has strong enforcement provisions to deter this practice, including civil penalties and the existing ERISA remedies. Congress should pass H.R. 306 as quickly as possible to end genetic discrimination in health insurance once and for all.

While it is extremely difficult to measure how many people may have been harmed by lack of medical privacy, Americans clearly believe such discrimination is already occurring. One study interviewed 332 people who belonged to support groups for families with genetic disorders. Of this group, 25 percent believed they had been denied life insurance based on their disorder; 22 percent alleged they had been denied health insurance on the basis of genetic information; and 13 percent believed they had suffered employment discrimination on similar grounds.

With the advent of computerized records, the potential for malicious misuse of this information is truly appalling. In a widely publicized case, a Florida public health official was fired after allegedly mailing computer disks with the names of thousands of Florida patients with HIV and AIDS anonymously to Tampa-area newspapers. This individual reputedly took a list of the patients into a local bar and offered to help friends screen potential dates. Last summer the *Baltimore Sun* reported that in Maryland alone, there have been examples of state employees accepting bribes from HMOs for information on Medicaid recipients. One banker obtained a list of cancer patients, cross-referenced it with loan customers at his bank and called in those loans.

There is a clear and pressing need for federal legislation to protect the privacy of our medical records. In a recent review of state medical privacy and confidentiality laws prepared for the Centers for Disease Control, the Electronic Privacy and Information Center (EPIC) called federal privacy laws "fragmented and uncertain." *The American Bar Association Journal* stated in an April article, "Few laws protect intrusions on genetic privacy despite the personal nature of the information. . . . Despite [privacy and other] concerns, the law generally has upheld third-party access to a person's genetic information on a number of fronts."

As long ago as 1994, the Institute of Medicine endorsed passage of comprehensive federal legislation to replace the patchwork of laws that cover medical records. According to the Electronic Privacy and Information Center's report,

Thirty-seven states impose on physicians the duty to maintain the confidentiality of medical records. Twenty-six extend this duty to other health care providers. Thirty-three states and territories require health care institutions to maintain the confidentiality of

medical records they hold. The survey found that only four states have specific legislation imposing this duty on insurers, despite the vast amount of information held by insurance companies. Nine states impose a similar duty on employers or other non-health care institutions.

..Only twenty-two states have legislative provisions that protect computerized or electronically transferred data. Forty-two states protect information received during the course of a physician-patient relationship from disclosure in court proceedings, with certain exceptions. ..Twenty-eight states provide statutory penalties for unauthorized disclosure of health care information. Twelve impose criminal penalties, nineteen create civil penalties and three allow for both civil and criminal penalties. *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization*, EPIC, February 1997.

The report concludes by endorsing passage of federal privacy legislation, stating, "Uniform standards nationwide will result in more effective protection of health information privacy."

The Genetic Information Nondiscrimination in Health Insurance Act would provide a desperately needed uniform standard. It applies to health plans regulated under the Employee Retirement Income Security Act (ERISA) as well as state-regulated, government, church, and individual plans. My legislation would resolve the current diverse laws and standards into a single, sensible statute.

The lack of federal privacy protections has major consequences for individuals in their everyday life. H.R. 306 has been endorsed by over 65 consumer, health, and provider organizations. For example, overwhelming numbers of Ashkenazi Jewish women fear they are at increased risk for breast cancer due to the prevalence of the BRCA1 gene in this population. However, growing numbers are deciding not to take a genetic test because they are afraid they will be subject to health insurance discrimination if it comes back positive. In fact, some Jewish women's groups are now actively discouraging their members from taking genetic tests for this very reason.

Concern over genetic discrimination is not limited to just breast cancer victims, however. It affects every one of us. No one has a perfect set of genes. Sooner or later, science will be able to tell each of us that we are predisposed to a handful of disorders. We should not feel compelled to deny ourselves this information, or shun the science that reveals it, simply because we fear genetic discrimination from health insurers. It is tragic that Congress is allowing a situation to persist in which Americans are forced to choose between knowing information vital to their health, and risking their health insurance.

Once again, Mr. Chairman, I commend you and the subcommittee for taking on this complex and daunting issue. Despite the hurdles we face, strong protection of medical records is vital to the future of health care and medical research in our nation. I look forward to working with you to ensure that any bill considered by your subcommittee or the House of Representatives contains strong protections for genetic information and prohibitions against genetic discrimination.

Mr. HORN. Let us now, in your limited time, ask a few questions. Given the situation on genetic information in those cases, Representative Stearns, that you cited, are truly important because I happen to have a college classmate whose child had exactly that heart situation. No one thought the child would live past 8, and that child is now in his late 30's or early 40's. So genetic information doesn't always have an inevitable consequence.

And I think the one question here is, should we separate the genetic information aspect from the other privacy aspects in the Condit bill, or should we just work on both in one piece? What is your feeling on that?

Mr. STEARNS. Well, I think what Gary is doing is important, and I think separating them temporarily until we know enough about it—because as you just pointed out, if a doctor sits down with me and says, Cliff, you have a predisposition because of your gene for X, Y, Z, what does that mean in terms of probability theory? Does the environment, the fact I don't drink or smoke or perhaps that I exercise, perhaps where I live, how does that tie in? And what does that predisposition mean? We just don't know.

We can say, in some genes, it means you are going to die at a definite date. But for a lot of this, there is going to be a high level of probability that we have to work out and we should not have the health records impeded while we try to understand the whole impact of this, in the legal aspect, in terms of punitive—allowing research to go ahead, in terms of counseling people. I mean, the issues just open up like Pandora's box.

So I think the whole area of genetics is an issue unto itself in how we deal with it, much like we are trying to deal with cloning. And as you know, the President's Commission, I think is going to reveal its recommendations this week or next. And so this whole area is something that is staggering in terms of implication.

Mr. CONDIT. May I respond?

As you know, you and I have had discussions, we are looking for a comprehensive approach to medical records and the confidentiality, and so we would like to eventually see everything sort of on an even keel here. But I do acknowledge that what Mr. Stearns has brought up here is sort of in a special category. At this time, we don't have a lot of information about it, so I do think that there is a time period where we may want to do as he said, take a special look at it and see whether or not it fits under this category. But we probably could work to accommodate it either way, but I think he makes a very good point and one we would probably agree with.

I also, Mr. Chairman—if I may, I apologize to you; you have been very kind to hold this hearing today, and I know you are going to get a lot of good information. I have another obligation I need to get to, but I do have a stack of information I would like to leave for the record, if I may.

Mr. HORN. Without objection, it will be inserted at this point.

I just have one question, if you have got a second.

On H.R. 52, as put in this year, is there an impact on law enforcement investigations? I recall that some law enforcement officials, representatives of the Department of Justice, in particular, expressed concern about your previous legislation, H.R. 435, and its

effect on law enforcement investigations. Do you know of any similar concerns?

Mr. CONDIT. That is a good point, and I am glad you brought it up.

It is certainly not my intent to exclude law enforcement from having access to information that is crucial to them, maybe in a criminal case. So last session when we worked on this issue, we spent a lot of time working with the law enforcement industry, and I think we clarified, to their satisfaction, language that they can accept. And I think they are protected under this bill, and we have not received, to my knowledge, any objection from them on this particular language. They do have access to records when they need them.

Mr. HORN. Thank you very much.

Mr. Stearns, when I listened to your examples on genetics and how insurance companies were doing this and that, it came to my mind that the whole reason we have insurance is not just to insure well people, but to insure a group of people, and that is what the actuarial tables, it seems to me, are based upon; and to deny an individual, just because science has progressed, it bothers me a lot, and we have to do something to figure out how to solve that one.

Do you have any other comments you want to make? I don't want to hold you here. I know you have a lot of things to do.

Mr. STEARNS. Well, Mr. Chairman, in the area of law enforcement, also in the area of military, that is another area that health records—in determining availability, access for military people, military doctors, putting people in combat; and with genetic predisposition, how does that work out if a person has strong allergies or a person has some other problems that would become apparent under stress or would become apparent under certain conditions? How does that work out, and how is the individual protected, and what does it mean? That is an area that we need to have the wisdom of Solomon to figure out how to protect health records and at the same time allow the military, the law enforcement and research—most importantly, research—to have access to the records.

So, I mean, it is something I commend you and others for doing, and I am delighted to be here.

Mr. HORN. Let me just ask if Mr. Sessions has any questions he would like to ask you before you leave.

Mr. SESSIONS. I really have no questions. I would just say that I was unprepared before I walked in today. I knew the general subject. I have a little boy with Down's Syndrome, so I have had to ask a lot of these same questions, not only of myself in dealing with him, but also of my son, and how we are going to deal with him as he progresses.

So these are very thought-provoking issues, and I am very interested in your comments today and those of Congressman Condit.

Mr. STEARNS. Dr. Collins, who heads up the Genome Project out at the National Institutes of Health—I went out there and toured the facility, and I urge all Members to go out there and to actually meet with Dr. Collins and hear his presentation on the future with genetic engineering. It is exciting.

For example, with your son and other children that many Americans will have, the hope some day is we can actually go back into

your DNA and correct things and make things new again, and that is a spectacular kind of thought. But at the same time, for many Americans who have mutated genes, we need to make sure that they have a full life and are not discriminated against because of anything that medicine finds.

Mr. SESSIONS. What is interesting to me, since we are on the subject—and I know you need to go—I struggle and I have struggled in dealing with my child. Many people, in dealing with all sorts of gene and genetic problems, as Down's Syndrome is one of those, I am of a firm belief that God gave us baby Alex the way he is, and we are simply trying to take him as far as we can; and a lot of changes, I would not want to make to him. We are trying to take him as far as he can go as he was given to us.

And a lot of people do things with exercise or their facial muscles so that the disability that this child has is not recognizable. And so my wife and I have taken the perspective in dealing with this that we want to massage him, we want to do those things that help his facial muscles, that help him to be able to speak and help him to do those things, but he should not become unrecognizable for what he is to this world. He could, at some point, be 25 years old on a street corner, be lost, and a person would look at him and maybe not know what they are looking at.

So I have found that I like baby Alex the way he is, and he was a gift to us; and I would not go back and alter one single thing, even if I knew he were Down's from the very beginning. So there are a lot of things that come to us that may not be exactly the way you and I think are perfect, but is in reality a wonderful creation.

Mr. STEARNS. Well, that is an inspiring attitude toward it, and I think all of us should have that attitude on many things. So I commend you for that attitude, and I think that is an inspiration for many of us.

Mr. SESSIONS. Thank you.

Mr. HORN. I agree with the gentleman. When you mentioned allergies, the thought crossed my mind that no one on Capitol Hill would be able to get insurance. As I walk down the hall, everybody seems to have allergies. And when our class arrived in the fall of 1992, somebody said, you know, "Why we all have allergies?" We apparently have one of every tree in America on Capitol Hill. I don't know if it is true, but it is an interesting source for what the problem is around here.

Would the gentlewoman from New York care to ask any questions?

Mrs. MALONEY. I would like to have my opening comments put into the record as read.

Mr. HORN. That has automatically been done already.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

**Opening Statement of  
The Honorable Carolyn B. Maloney on  
The Privacy of Medical Records**

**June 5, 1997**

**Thank you, Mr. Chairman, for holding this important hearing. Congress has been struggling with this issue since the President first proposed his sweeping health care reform four years ago. There have been more bills on this issue than I care to remember, and each one has faded away.**

**It is easy to get lost in the intricacies of these bills. Who gets access to the information and when? When do you require patient consent to release information, and when can it be done automatically? What happens in an emergency? How do we make provisions for research, and so on?**

**What gets lost all too quickly in these discussions is the very real fact that right now there is NO federal protection for medical information, and peoples privacy is routinely violated. Every day we yield to the special interests that have kept this legislation bottled up, more people get hurt.**

**Four years ago, during a congressional campaign, one of our colleagues was confronted with an ad by her opponent that used her medical records to question her qualification for office.**

Every day, people are denied employment because of their health. Every day, insurance companies use what should be private medical records to deny coverage. One insurance company in bidding on coverage went back to the employer and said they would cover all of the employees but one. Her problem was that her husband abused her, and the insurance company decided she would cost too much.

In a few minutes we will hear from Congresswoman Slaughter about her bill on genetic information and health care. She will tell a similar story of what should be private information being used to deny health insurance. I am proud to be a cosponsor of her bill, and I hope that this Congress will take it up quickly. If not, Mr. Chairman, I hope you will work with me to incorporate the principles of her bill in anything that we do in this committee.

I would like welcome all of our colleagues who are going to testify today. We are fortunate to have the opportunity to receive advice from such a talented group of members. I would like to extend a special welcome to our colleague Rep. Condit whose bill we are considering today. Without his leadership on this issue in the 103rd Congress we would not be as far along as we are today.

Again, thank you Mr. Chairman for holding this hearing, and I look forward to working with you to pass a bill that protects the public from the misuse of their medical information.

Mrs. MALONEY. I am sorry Mr. Condit has already left. We wouldn't be as far along as we are on this issue if it had not been for the work he did in the 103d Congress.

I wanted to ask him, but maybe Mr. Stearns can answer, in one of his bills, he had exempted mental health, and yet now he dropped from his bill the exception for mental health treatment, and I wanted to ask him why. Are you working with him on his bill?

Mr. STEARNS. No, I am not and it would not be fair for me to comment on his bill. Gary is very knowledgeable.

Mrs. MALONEY. Do you think the provisions in Congresswoman Slaughter's bill are adequate or would you add to them?

Mr. STEARNS. Well, this is a bill that we dropped pretty much like we dropped last year. Senator Mack and Senator Hatfield dropped it on the Senate side.

The bill we are going to drop this year is going to be a little different, and we think that our bill is going to be more specific and tailored. And we are seeking the administration's help, because we think the administration has some concern about certain things; and since we are trying to get something passed, we are trying to work with them.

She has also been very active, and I admire her for her leadership and her activities on this, and welcome the work that she has done and working with her.

Mrs. MALONEY. OK. Thank you very much.

Mr. HORN. Thank you for coming. We appreciate you having shared your knowledge on the subject. When will that task force of yours report, basically?

Mr. STEARNS. Mr. Chairman, Gene Green of Texas represents Houston. We are hoping to have some hearings at some of the universities. University of Florida has a lot of research on this and we are hoping to have a hearing in July, in which we try to define where in this enormous panoramic subject that we could go and get the most bang for the buck. We would seek your advice and the members of this committee too.

Mr. HORN. Well, we thank you for the hard work you have dedicated to this issue. It is very important.

We will now call forth the second panel, and that will be Ms. Goldman, Mr. Palmisano, and Ms. Johns.

If you stand and raise your right hands, we have a tradition that witnesses other than Members of Congress take the oath.

[Witnesses sworn.]

Mr. HORN. All three witnesses affirmed, and we will start with Ms. Goldman.

**STATEMENTS OF JANLORI GOLDMAN, VISITING SCHOLAR, GEORGETOWN UNIVERSITY LAW CENTER, AND AFFILIATED WITH THE CENTER FOR DEMOCRACY AND TECHNOLOGY; DR. DONALD J. PALMISANO, MEMBER, BOARD OF TRUSTEES, AMERICAN MEDICAL ASSOCIATION; AND MERIDA L. JOHNS, Ph.D., PRESIDENT, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION**

Ms. GOLDMAN. Good morning, and thank you very much for inviting me to testify today. I not only appreciate your invitation, I

appreciate this subcommittee's continued commitment to this issue. I think this might be the third or fourth hearing on this subject you have held in the last few years, and I think it has advanced the policy discussions quite a bit.

What I would like to do, since this has been an issue that has been very well discussed and documented—there is quite a record that this subcommittee alone has created—is just talk a little bit about what has changed since the last hearing, which was almost a year ago today. Congress passed the Health Information Portability Act, the Kassebaum-Kennedy bill that now—really what Congress did, in place of passing mandatory privacy rules, was give itself a time limit and say, we must act to pass legislation in the next few years on privacy of health records, or else the Secretary of HHS will promulgate regulations. So one way or another we are going to have a law on enforceable regulations in the next few years.

It was, I think, a serious failing in the Kassebaum-Kennedy law that the administrative simplification provisions did pass, which require standard uniform format of health information, essentially a computerized patient record in the next few years, without saying at the outset what the privacy rules should be.

What it means is that as the Secretary and as the computer industry and the health information industry is moving to computerize and standardize personal medical records, they are doing so without knowing what privacy and security rules to put in place. So when Congress does act or the Secretary acts, they are going to have to go back and retrofit those systems.

It is expensive. I think it is a problem. I would urge the Congress not to wait until the time limit it has been given, but to act more swiftly so that people who are in those offices, in those industries, that are working with health information, know what to do at the outset.

In that law though that did pass, instead of passing the rules, what Congress did do was say, we need to address the privacy issues. A committee was created, the National Committee on Vital and Health Statistics. It has held hearings on the issue and created an even more extensive public record about the need for health privacy legislation. The Secretary is going to issue a report this summer.

In addition, since last year, the National Research Council issued a report for the record, very detailed report about the need for security in computerized health information systems. They went around the country, they did case studies and they found that even with the best of intentions, there was a lack of strong privacy and security safeguards in place. And again we have horror stories about people who acted with malice and used information without permission, sold it to the press. We have information about carelessness, we have horror stories, but I think for the vast majority of people in this country who want to do the right thing, they don't know where to start and they are seeking Congress' guidance.

As well, the National Action Plan on Breast Cancer and the Human Genome Project, which we have talked a little bit about, is holding a series of workshops on privacy and genetic information, because they are wrestling with the need to push forward in

genetic research. But the fear that so many individuals who are participants in these studies are going to have, is fear that they will be discriminated against in insurance, even in employment. Even though the ADA should protect them against that, they do not trust the research and public health community to protect their confidentiality.

I don't think it is an overstatement to say we are rapidly, and have been for years, approaching a crisis in health care because of the lack of privacy rules. Fundamental critical health care services are at risk of being undermined.

This is not a case of privacy practices being a barrier to research and to public health and to managed care; that is often how the issue is formulated in the press and by some in the industry who say, "privacy will be a barrier to us, if we have to protect privacy, we are not going to get the information we need because people won't consent to these uses."

I would actually say we have quite the opposite scenario. We will have substantial barriers to treatment, research, and public health if people do not believe that their privacy is protected and that they don't have the following principles guaranteed.

One is, they must have access to their own records. Half the States in this country give people the right to see their own medical records. It is a sham.

The other thing people must have is control over their own records. When they go to a doctor, they should be able to determine who else gets to see the record and under what circumstances. Right now people sign blanket waivers, and even where doctors want to maintain confidentiality and want to have kind of the old-fashioned doctor-patient relationship, they are unable to do so because of requirements on the part of payers, insurance companies, sometimes researchers with whom they have relationships, to disclose that information.

The other thing people must have are strong enforceable remedies, individual remedies where they can pursue a lawsuit against someone who has harmed them. There should be civil penalties and criminal penalties. Most of the legislation that has been introduced in both the House and the Senate has very strong penalties.

Very quickly, on some of the issues raised, my view—and, I think, the view of a number of people in the research community at NIH in the Human Genome Project—is that we should treat genetic information as health information and not treat it separately and not isolate it as a separate, special circumstance. In fact, H.R. 52, Congressman Condit's bill, does incorporate genetic information now under the definition of personal health information. It talks about past, present, or future information, as do a number of the Senate proposals. That is genetic information. It refers to information about others who are not necessarily the record subject. That is also genetic information.

As well, I think that the law enforcement provisions, which I know and, Mr. Chairman, you raised in your questions, I really believe that the law enforcement sections in a health privacy law must be consistent with other law enforcement provisions and privacy laws that we currently have at the Federal level.

The Video Privacy Protection Act, better known as the Bork bill by some, the Right to Financial Privacy Act, the Education Privacy Act, all have law enforcement provisions that require a warrant before access; and I think that we should have at least the same level of protection for medical records that we have for video rental records.

In addition, the pre-emption section which is in H.R. 52 is different than some of the provisions on the Senate side, but I think also needs some looking. Right now, we can't do any worse than we currently have since there is no Federal standard.

Again let's look at the very serious consequences. Without privacy protections, people are going to withhold information from their doctors because they are going to be afraid the doctor will have to convey it to somebody else, and they know the protections aren't in place. They will withhold information or they may lie to their doctors; they may give inaccurate information, which will undermine the ability of the doctor to give an accurate diagnosis. The other problem is that doctors may actually lie in submitting the claim forms, and I don't mean to suggest doctors are doing ill here, but they are trying to protect their patients, so they often put inaccurate diagnoses on the claim forms.

Or I think the more horrible consequence is that people will not seek health care. They will stay away from health care altogether because of fear, and we see it in the HIV area and reproductive health; people are afraid of going to the doctor at all in terms of discrimination and employment and insurance, that their families may find out, reporters, marketers. The personal consequences are very real, but I think the societal consequences are even more startling and one that we tend to overlook, which is that public health will be undermined if we don't have accurate information; and research will be undermined if we don't have accurate and reliable information.

So while the public health people and researchers often say we are worried about how privacy rules will affect our work in improving health care, we really need to look at the cost of not protecting privacy. Privacy, I believe, is a necessary, vital partner in other health care goals. It is not a barrier, it is not an impediment, but it is a partner in achieving other health care goals.

I appreciate your holding this hearing. Thank you.

Mr. HORN. We thank you for the most helpful statement.

[Note.—A copy of the report entitled, "Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality," can be found in subcommittee files, and may be obtained by calling (206) 682-2811.]

Mr. HORN. Dr. Palmisano, member of the Board of Trustees of the American Medical Association.

Dr. PALMISANO. Thank you Mr. Chairman and members of the committee. My name is Donald Palmisano, and I am here representing the American Medical Association and some 300,000 physicians and medical student members. I also bring to the discussion today my 26 years' experience as a surgeon practicing in New Orleans. We appreciate the time and energy the subcommittee is devoting to this important issue.

Let me begin by stating medicine's underlying premise in all of the discussions of patient confidentiality. The patient-physician relationship is first built on trust. Confidentiality of communications within this relationship is the cornerstone of good medical practice and good medical care. Patients must feel safe in disclosing to their physicians personal and sometimes embarrassing facts and information that they do not want others to know. We, as physicians, need this information to provide the best and most appropriate medical care. Without such assurances, patients may not provide the information necessary for proper diagnosis and treatment. The cost of medical care can increase when physicians do not have such information.

Our professional and ethical responsibility is outlined in our AMA Code of Medical Ethics and it is to keep our patients' confidences, and it is no different because the medical records are stored electronically rather than on paper. But the evolution of electronic medical data has intensified our existing concerns about access to and, now, even commerce in patients' confidential medical information.

The growing number of third parties demanding information has eroded our patients' confidence that information that they share with their doctor is going to help in their individual care. Any number of parties will give you arguments for a vast array of supposedly compelling health and public safety reasons as to why they need to know such private information.

But a need is not a right, and I would like to emphasize that, a need is not a right. And because it may be happening now, doesn't make it right.

AMA policy clearly states that conflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of the patient except where that would result in serious health hazard or harm to the patient, or others; and we would suggest that all bills studied in the Congress use that guideline so that the patient is the primary protector of his or her own medical information, and not someone else's right, desire, or belief in their right to get that information.

We believe that patients have a basic right of privacy of their medical information and records. We believe that the patient's privacy should be honored, unless the patient waives it in a meaningful way or in rare instances of strongly countervailing public interests. And by "meaningful," we mean informed and not coerced.

We believe that you should limit the information disclosed to that part of the medical record or abstract necessary to fulfill the immediate and specific purpose—that is, no fishing expeditions.

While you have our written statement, which goes into more detail, I would like to highlight a few points. First, we cannot forget that the primary purpose of the medical record is to provide a reliable tool and to provide clinical diagnosis and treatment for patients. Patients should generally have access to information from their medical record. There are few exceptions to protect the mental or physical safety of the patient, but the physical record is the property of the physician or provider, and this is where control of most disclosures should emanate.

Second, on the issue of consent, a patient's first consent, generally for treatment or payment, should not automatically apply to subsequent disclosures unless the patient specifically and freely waives defined rights. Insurers, of course, need basic information to pay claims and have legitimate need for information to conduct utilization review and quality assurance and to monitor for fraud and abuse. The AMA cautions against categorizing these activities as payment for treatment purposes when they do not go directly to paying for a specific individual's treatment.

Patients generally believe that their signature releases personal information for their direct and specific benefit, overly broad and legislative definitions should not exploit patients' lack of knowledge regarding complex information systems. For consent to be truly voluntary, it must be knowing and that includes a patient knowing for what purpose their records are being sought. Patients should not be coerced into divulging any and all medical records, either their own or their families by way of a nonspecific consent signed upon enrolling in a plan as a condition of insurance payment, nor should physicians have to sign agreements with insurers to produce records without that patient's consent.

Third, exceptions to the requirement for patient consent to disclosure should be minimally and narrowly drawn.

Last, whenever possible, medical information used for research purposes should have all identifying information removed, unless the patient specifically consents to the use of his or her personally identifiable information.

In conclusion, the fact that we have vastly improved technology to collect, sort and analyze patients' medical data does not diminish our ethical obligation to protect our patients' privacy. We all hear seemingly compelling arguments for efficiency and technological potential, but we cannot allow the vigorous standards of confidentiality required by the medical profession's ethical code to be subverted once the record gets into others' hands. We have to work to fit the goal of efficiency within the larger framework of patient privacy, not the other way around.

Thank you again for inviting the American Medical Association to testify. I am happy to discuss our testimony in more detail, and the AMA is happy to work with the subcommittee to address concerns. Thank you very much, sir.

Mr. HORN. We thank you. That is a very well developed statement, as I read it earlier.

[The prepared statement of Dr. Palmisano follows:]

**STATEMENT**

**of the**

**American Medical Association**

**to the**

**Subcommittee on Government Management, Information and Technology  
of the House Committee on Government Reform and Oversight**

**Presented by**

**Donald J. Palmisano, MD, JD  
Member, AMA Board of Trustees**

**RE: MEDICAL RECORDS PRIVACY**

**June 5, 1997**

Mr. Chairman and Members of the Subcommittee, my name is Donald J. Palmisano, MD, JD. I am a member of the Board of Trustees of the American Medical Association (AMA) and practice vascular and general surgery in New Orleans, Louisiana. On behalf of the approximately three hundred thousand physician and medical student members of the AMA, I appreciate the chance to comment on the issue of medical records confidentiality and thank the Subcommittee for devoting the time to discuss this important issue.

The patient-physician relationship is based first on trust. The AMA believes that the confidentiality of communications within this relationship is the cornerstone of good medical care. It cannot be too strongly stated that in order for physicians to provide the best and most appropriate medical care, patients must feel that they can disclose to their physicians personal facts and information that they would not want others to know. Without such assurances, patients may not provide the information necessary for proper diagnosis and treatment.

The evolution of electronic medical data has intensified existing concerns about access to patients' confidential medical information. Concerns regarding the transmission and aggregation of electronic data and the growth of supportive infrastructures are amplified by the ease of split-second data cross-referencing and "linkages" to other information databases.

The confidential relationship between patient and physician has been eroded by growing outside demands for the information that is shared within this relationship for the purpose of patient care. The "need to know" such private information has been loosely established for any number of outside parties who present arguments for a vast array of compelling health and public safety reasons. But, needs do not bestow rights. AMA policy clearly states that "conflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of the patient, except where that would result in serious health hazard or harm to the patient or others." (Policy 140.989)

The AMA's analysis of the issue is based on a threefold premise:

- that there exists a basic right of patients to privacy of their medical information and records, and that this right should be explicitly acknowledged;
- that patients' privacy should be honored unless waived by the patient in a meaningful way (i.e., informed, noncoercive) or in rare instances of strongly countervailing public interest; and
- that information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose (i.e., no fishing expeditions).

Within the context of these three overriding principles, the AMA offers the following recommendations by which any medical information or record confidentiality legislation, including H.R. 52 currently before this Subcommittee, should be assessed:

1. **The primary purpose of the medical record is to provide a reliable tool to provide clinical diagnosis and treatment of patients.** The medical record is the property of the physician or responsible health care provider or entity, who has legal and ethical obligations to maintain a true and accurate record. While patients should have access to the information from the medical record (with rare exceptions to protect the mental or physical safety of the patient), the physical record is the property of the physician or provider. When a provider entity controls the medical records or information, a physician advisory body to the provider (or a medical staff if one exists) should superintend the manner in which the physical record is released.

Regarding the disclosure and correction of patient records, the model of the procedures for reporting and correcting consumer credit information is not translatable to the medical information arena and should not be adopted without significant modifications acknowledging this distinction. Subsequent holders of medical information (such as information data banks or other types of "trustees") should not be allowed to change medical information or conclusions. It follows that, if at all possible, the treating

physician or health care practitioner that generated the medical information should be the only "trustee" through whom patients may "amend" or "correct" their medical information or records.

2. **"Firewalls" should be constructed so as to preclude a patient's first consent from applying to all subsequent disclosures (unless the patient specifically and freely waives defined rights).** The specificity of the patient's consent creates the "firewall." Requests for information should be specific as to, for example:

- the portion of the records or information needed (the specific treatment or condition at issue);
- the time period of the records needed (e.g., "from May 1996 through the present"); and
- the purpose for which the information is requested.

The specificity of consent is the key to imposing effective "firewalls," to preclude the lateral drift of information once an initial consent is agreed to by the patient. Patients and physicians will feel more protected if a signed consent is required for each disclosure or category of disclosure of records, rather than to continue to allow for blanket waivers by patients. Blanket authorizations may be acceptable for most treatment and payment purposes and for the release of "de-identified" charts; however redisclosure of individually identifiable medical information, as a rule, should be prohibited without initial or subsequent authorization. In instances where personally identifiable medical information is part of a requested record that is not easily "de-identified," specific permission from the patients should be obtained. The responsibility for obtaining consent for disclosure should rest with the entity requesting the data.

For consent to be truly voluntary, it must be knowing. Patients should not be coerced into divulging "any and all" medical records, by way of a nonspecific "consent" signed upon enrolling in a plan, as a condition of insurance payment (this is true for the individual, as well as his or her dependents); nor should physicians have to sign agreements with insurers to produce a patient's records without that patient's consent.

Insurers, of course, need basic information to pay claims. They also have legitimate needs for information to conduct utilization review and quality assurance, and to monitor for fraud and abuse. The AMA cautions against categorizing these activities as "payment or treatment purposes," when they do not go directly to paying for a specific individual's treatment. Patients generally believe that their signature releases personal information for their direct and specific benefit; overly-broad legislative definitions should not exploit patients' lack of knowledge regarding complex information systems.

3. **Legislative exceptions to the requirement for patient consent to disclosure should be minimal and narrowly drawn.** The burden should be on the requesting entity to demonstrate why its need should override the patient's confidentiality. This burden should be equally applicable for research (both scientific and market-based/economic), law enforcement and any other legitimate purpose.

In the particular instance of exceptions for purposes of law enforcement, the AMA believes any legislation should set high standards for non-consented-to disclosures. The AMA recognizes the needs of legitimate law enforcement; however, these needs must be balanced with an individual's expectation of privacy for his or her personally identifiable medical information. The requesting entity should be required to show, at a minimum, "probable cause" in establishing why medical records should be divulged without the patient's consent and that the information sought is not otherwise available. The particular information required to meet the immediate law enforcement purpose should be specified. Records thus disclosed for legitimate law enforcement purposes should then be subject to security measures, such as being held *in camera* by the court.

4. **Whenever possible, medical information used for research purposes should have all identifying information removed, unless the patient specifically consents to the use of his or her personally identifiable information.** Most "research" and quality assurance activities can be performed using de-identified data, generally in the aggregate. When that is not the case, the entity requesting protected medical records or information should be required to pay for "de-identifying" the record. Ideally, patient identifying information should be removed by the physician or provider; in any event, this activity should be segregated from the entity wishing to use the information.

The AMA is generally satisfied that the protections relating to release of identifiable information without authorization when a federally recognized institutional review board (IRB) determines that the need for that information outweighs the individual's right to privacy are adequate without further showing of problems that might currently exist.

"Research," in particular, is a troublesome category of exceptions to the general requirement for patient consent to disclosures. "Research" has been used as a comprehensive term to cover a spectrum of activities, ranging from purely medical and scientific, to purely economic analysis. To no one's surprise, the legislative goal of many of the entities desiring access to confidential information is to have one's activities categorized in the most benign manner so as to qualify for the broadest exception accompanied by the least restrictive use of private information.

5. **Without a showing that the proposed federal standard would be properly protective of patient privacy, any federal law should provide a "floor," rather than a "ceiling" when applied to patient confidentiality protections.** It is understood that there are many who believe that there should be a uniform federal standard to facilitate electronic data interchange. The AMA is concerned, however, that heightened state standards will be lost to federal legislation. If, however, the bar is placed high enough to

secure protection of patient information in the federal language, the AMA would revisit the preemption issue.

6. The AMA believes that **penalties and sanctions for unintentional disclosures of identifiable patient information, where the disclosure does not result in demonstrable harm to the subject of the disclosure, should be commensurate with the violation. Repeated such unintentional disclosures should receive stronger penalties, if they indicate a negligent business practice. Penalties and sanctions related to improper disclosure for commercial purposes, profit, malicious purposes or where there is significant patient harm should be most stringent.** In addition to monetary sanctions, legislation could include the loss by a database company, for example, of its privilege to hold or transmit protected medical information, thus reducing the potential for companies to accept the monetary penalties for improper, intentional disclosures as a "cost of doing business."

#### **Conclusion**

The fact that we have vastly improved technology to collect, sort and analyze patients' medical data does not diminish our ethical obligation to protect our patients' privacy. Neither "efficiency" nor "technological potential" are compelling enough arguments to allow ourselves to be seduced away from the rigorous standards of confidentiality required by the medical profession's ethical code.

Finding the proper balance between individual rights and the public good is the continuing challenge of our democracy; it is no easier here than in the many other issues before the Congress. The AMA appreciates the chance to share our principles with the Subcommittee and is ready to provide continued assistance as this complex issue moves forward.

Mr. HORN. Dr. Johns is President of the American Health Information Management Association, a rather large organization. Give us a little bit about its history. I know you mentioned the numbers in your second paragraph, but I think you could educate most of us about the extent of your membership.

Ms. JOHNS. I will be happy to, Mr. Chairman.

Thank you, Mr. Chairman and members of the subcommittee. AHIMA appreciates the opportunity to appear before the subcommittee today in support of the Fair Health Information Practices Act. AHIMA is an organization that was established 69 years ago and a professional organization that represents 37,000 credentialed health information managers. We have over 200 educational programs throughout the country, in colleges and universities which prepare accredited record technicians and record administrators.

Our organization, a professional organization, was originally established for the purpose of managing, storing, and protecting health information, and we have a long tradition with the issues regarding confidentiality and privacy, and a principal goal in the mission of our organization, since 1929, for protection of health information. So certainly, we are not new to the issues that are being posed today.

We are the credentialed specialists who manage and protect patient health information. We work in a variety of health care institutions and health-related organizations, and we are the professionals that are responsible for handling requests for information from third-party payers, from employers, from researchers, attorneys, other health care providers, local, State, and Federal agencies. Our members ensure that information is disclosed pursuant to valid authorizations and pursuant to statutes, regulations, and court orders. Our efforts, however, to protect health information have been complicated by a lack of Federal pre-emptive confidentiality legislation.

Assuring confidentiality is important because it makes patients feel comfortable enough to communicate openly with their health care providers. Assuring confidentiality is also important because it makes patients feel comfortable that the information they are providing health care providers is going to be protected. Unfortunately, current regulations and the physician-patient privilege do not offer patients real protection. Therefore, AHIMA believes H.R. 52 is a solution to this dilemma, first, because the bill establishes a code of fair information practices, and, second, because it provides a uniform national health standard for the use and the disclosure of individually identifiable health information.

It is true that some States have enacted confidentiality legislation, but there is little uniformity with their approaches. Most statutes do not even address the issue of redisclosure of health information, and penalties for its misuse are lacking. Protections also vary according to the holder of the information, and for different types of information.

For instance, several States have recently enacted genetic privacy legislation. Segregating and creating special protections for specific types of information, such as mental health or genetic information could result in inadvertent breaches of confidentiality.

For that reason, AHIMA recommends that comprehensive confidentiality legislation cover all types of health information.

One of the greatest threats to patient privacy is the increasing and growing demand for data, and while there are Federal regulations that offer strong protections, they are limited in their applicability. For example, the Federal Privacy Act of 1974 was designed to provide citizens some control over the information collected on them by the Federal Government. However, this law does not apply to the private sector. There are also Federal regulations in regard to alcohol and substance abuse, but these only apply to Federal or federally funded facilities that offer treatment for alcohol or substance abuse.

As a result of the ongoing public policy debate, during the past several years, Congress and the general public have come to a consensus there is a need for Federal confidentiality legislation. Reports of the Institutes of Medicine and from the Office of Technology Assessment and, most recently, the National Research Council have all underscored the need for Federal action.

In order to address the need for Federal legislation, AHIMA in 1993 drafted model legislative language that outlined a code of fair health information practices. This language was published in the Office of Technology Assessment report, protecting privacy in computerized medical information as a model code, and was used in drafting the Fair Health Information Practices Act.

There are a number of key provisions in the model language that are essential to any legislation governing the collection, use and disclosure of health information. These include, first, a patient's right to know and access his or her own health information; the provision—providing provisions for restrictions on information used and provisions for criminal and civil penalties to protect the misuse of information. We are pleased to note that H.R. 52 covers all of these key provisions.

We are also pleased to note that H.R. 52, in sections 101 and 102, provides individuals with the right to access and copy the personal health information and also to amend errors as well. Currently, only 28 States allow patients access to their health information, and even within these particular statutes, they are not uniform.

We note, however, one principal concern with sections 101 and 102. These require health information trustees such as health benefit plan sponsors, health care providers, health oversight agencies and public health authorities to permit patients to inspect and copy their records. They also require that these trustees correct or amend protected health information upon request, or take certain actions if they refuse to make such changes.

Because medical records are the physician's or health care facility's legal record, they are an important element of patient care, and we urge that the language be amended that only providers be permitted to correct health information. In other words, information should be corrected at its source.

AHIMA believes that the passage of pre-emptive confidentiality legislation is imperative, and we thank the subcommittee for holding this very important hearing. We sincerely hope that our testimony will prove helpful. In addition to the points we have made

here today, we would be more than willing to offer our technical comments to you, as you continue to discuss the provisions of the Fair Health Information Practices Act.

[The prepared statement of Ms. Johns follows:]

Mr. Chairman and Members of the Subcommittee:

My name is Merida L. Johns, PhD, RRA and I am President of the American Health Information Management Association (AHIMA). AHIMA appreciates the opportunity to appear before the Subcommittee on Government Management, Information and Technology and to announce our strong support for the "Fair Health Information Practices Act of 1997 (HR 52)".

The American Health Information Management Association (AHIMA) is the professional association which represents over 37,000 credentialed specialists who, on a daily basis, manage and protect the health information that is an increasingly important component of our nation's health care delivery system.

AHIMA members work in health care organizations throughout the United States and ensure that an individual's right to privacy is protected. Health information management professionals handle requests for health information from third party payers, employers, researchers, attorneys, other health care providers and local, state and federal agencies. Our members ensure that information is disclosed pursuant to valid authorizations from the patient or their legal representative, or pursuant to statute, regulation or court order. This responsibility is not taken lightly and is complicated by the lack of uniform national guidelines or legislation.

For the past 69 years, AHIMA and its members have assumed the responsibility for protecting the confidentiality of health information. Our efforts have been complicated by the lack of federal preemptive legislation. AHIMA believes that the "Fair Health Information Practices Act" is a solution to this dilemma as the bill establishes a code of fair information practices and a uniform national standard for the use and disclosure of individually identifiable health information.

The primary goal of confidentiality is to allow patients to communicate with their physician and to share information regarding their health status. Trust is an essential element in the relationship between patients and health care providers. One of the most important aspects of this relationship is the provider's duty to maintain the confidentiality of health information. The historical origin of a physician's obligation, for example, is found in the Oath of Hippocrates, written between the sixth century B. C. and the first century A. D. The Oath states "what I may see or hear in the course of treatment in regard to the life of men, which on no account must spread abroad, I will keep to myself....." Ethical codes promulgated by associations of health care professionals have consistently recognized the importance of confidentiality. However, these codes do not address current issues regarding use and disclosure of health information.

While communications between patients and physicians are privileged in most states, the protection of these laws is very narrow. The privilege only applies when a physician is testifying in court or in related proceedings. Many of these laws include significant restrictions that further limit the availability of the privilege. The physician

patient privilege offers no real protection to patients regarding the confidentiality of their health information.

Increasing demands for data pose a growing threat to the patient's right to privacy. The Federal Privacy Act of 1974 was designed to provide private citizens some control over the information collected about them by the federal government. Health care facilities operated by the federal government, such as the Indian Health Service, Veterans Administration and Department of Defense, are bound by the Act's requirements regarding access, use and disclosure of health information. However, the provisions of this law do not apply to health information maintained in the private sector.

Federal alcohol and drug abuse regulations only apply to federal or federally funded facilities that offer treatment for alcohol or drug abuse. While these regulations offer strong protection, they are limited in applicability. Currently, there is no uniform national standard protecting the confidentiality of health information. The protection of health information is left to state law.

Currently, only 28 states allow patients access to their health information. However, these statutes are not uniform in their approaches. A review of these statutes reveals that in some states patients may only access hospital records, while in other states they may access both hospital and physician records. There is little uniformity among state statutes and regulations regarding confidentiality of health information. Protections vary according to the holder of the information and vary for different types of information.

Most statutes do not address redisclosure of health information and lack penalties for misuse or misappropriation. Several states have recently enacted legislation to address issues regarding genetic privacy. However, there is no uniformity in their approaches.

It has been recognized that there is a need for more uniformity among the 50 states. In recent years, the National Conference of Commissioners on Uniform State Laws developed the Uniform Health Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington, have enacted this model legislation. Clearly, efforts must be directed toward developing national standards on privacy and confidentiality.

#### **THE NEED FOR FEDERAL LEGISLATION**

Over the past several years, a consensus has emerged within Congress and among the general public regarding the need for federal legislation to address this important issue. The Office of Technology Assessment (OTA) report, Protecting Privacy in Computerized Medical Information, found that current laws, in general, do not provide consistent, comprehensive protection of health information confidentiality. Focusing on the impact of computer technology, the report concluded that computerization reduces some concerns about privacy of health information while increasing others. The OTA report highlights the need for enactment of a comprehensive federal privacy law.

The public's concern about the confidentiality of health information was reflected in a poll conducted by Louis A. Harris and Associates for Equifax, Inc. The results of the Health Information Privacy Survey 1993 found that fifty-six percent (56%) of the survey participants indicated strong support for comprehensive federal legislation to protect the privacy of medical records as a part of health care reform.

The survey also indicated a strong agreement on what should be included in national privacy legislation. Ninety-six percent (96%) believe federal legislation should designate all personal medical information as sensitive and impose severe penalties for unauthorized disclosure. Ninety-five percent (95%) favor legislation that addresses individuals' rights to access their medical records and creates procedures for updating and correcting those records.

In 1994, the Institute of Medicine released a report, Health Data in the Information Age: Use, Disclosure and Privacy, which recommends that federal preemptive legislation be enacted to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals.

The 1994 Equifax-Harris Consumer Privacy Survey focused on how members of the American public feel about having their medical records used for medical research and how safeguards would affect their opinions about such systems and uses. Among a list of 13 groups and organizations, doctors and nurses rank first in terms of the percentage of Americans who are "very confident" (43%) that this group properly handles personal and

confidential information. After hearing a description about how medical records are used by researchers to study the causes of disease, 41 % of those surveyed said that they would find it at least somewhat acceptable if their records were used for such research. If a federal law made it illegal for any medical researcher to disclose the identity or any identifiable details of a person whose health records had been used, 28% of those who were initially opposed to having their records used would change their positions. This would increase the acceptance of this practice to over half of those surveyed (58%).

In the final Office of Technology Assessment (OTA) report, Bringing Health Care Online: The Role of Information Technologies, the issues of privacy and confidentiality were identified as particularly important areas in dealing with health information. The report noted that if there is little confidence that an electronic medical information system will protect them, then providers and patients will be unwilling to use it. The report recommends that Congress establish federal legislation and regulation with regard to privacy and confidentiality of medical information, as well as storage media for medical records and electronic data standards for storage and transmission of medical information.

The 1995 Equifax-Harris Mid-Decade Consumer Privacy Survey indicates that the American people say they are strongly concerned about threats to their personal privacy but believe business is doing a better job than government in handling personal information. A majority (58%) also now believes that privacy protection in the year 2000 will remain at least as strong as it is today, if not improve. Americans appear more willing to take active roles in protecting their own privacy, with six out of 10 now reporting

instances where they have refused to provide requested information. This is an increase from 42% since 1990.

The survey focused on the benefits of a computer-based patient record system. The majority of survey respondents see the trend towards a computer-based patient record system as either "very" beneficial (40%) or "somewhat" beneficial (45%). In terms of the personal benefits that computer-based patient record systems might provide, the greatest importance is attached to the benefit that enables key medical information to be sent to physicians treating patients in emergency situations away from home. Some 86% of survey respondents said that this would be "very" important to them. Nearly seven in ten people (69%) also said that a more effective presentation of past medical experiences, test results, and conditions would be "very" important to them. Finally, the elimination of a need to complete detailed forms as a result of the automatic printing of a patient's medical records and payment information would be "very" important to 55% of the public.

The survey also found that the ability of administrators to "identify sub-standard doctors and poorly run health facilities," to "improve the detection and reduction of fraudulent claims by patients, doctors and hospitals," and to "reduce the cost of health care by improving the identification of waste and inefficiency" would be very important to 79%, 76% and 74%, of the public, respectively. Seventy-four percent say the ability of medical researchers to get better statistical data for studying the causes of diseases and testing new treatments" would be "very" important to them.

The importance of benefits provided by computer-based patient records notwithstanding, most people say they are either "very" concerned (33%) or "somewhat" concerned (41%) about the potential negative effects of such systems. With detailed privacy safeguards in place, most people (80%) say they would be willing to have their medical records in computerized systems. Respondents indicated that a detailed privacy code would inform patients how their records are used; set rules of confidentiality; make it possible for patients to see their medical records; keep those records separate from all other consumer databases; and ensure the records are not used for marketing products to consumers.

Virtually, all respondents (98%) believe that a "patient should be able to obtain a copy of the medical record maintained about him or her by a doctor or health facility." In response to a similar question asked in 1978, 91% of the public said that "people who want to should have the legal right to see their medical records held by their personal doctor and by a clinic or hospital."

As a result of the ongoing public policy debate, The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) requires the Secretary of Health and Human Services to submit detailed recommendations on standards with respect to the privacy of individually identifiable health information to the Congress in August 1997. These recommendations must address the rights that an individual who is a subject of individually identifiable health information should have, the procedures that should be

established for the exercise of such rights and the uses and disclosures of such information that should be authorized or required.

Under the Health Insurance Portability and Accountability Act, if legislation governing standards with respect to the privacy of individually identifiable health information is not enacted by August 1999, the Secretary of Health and Human Services is required to promulgate final regulations containing such standards by February 2000.

Additionally, there are implications for the United States as a result of the new European Union Data Privacy Directive and related policy and legal changes. In October 1995, the European Union adopted a "Directive on the Protection of Individuals with regard to the Processing of Personal Data and on Free Movement of Such Data". By October 1998, all 15 E. U. member states must bring their national laws into congruence with the directive. This directive applies to health data as well as to many other kinds of data.

There presently are five bills which have been introduced in the 105<sup>th</sup> Congress to address issues regarding genetic privacy and non-discrimination. AHIMA recommends that comprehensive confidentiality legislation that includes protections for genetic information be enacted. Segregating and creating special protections for specific types of information, (i.e. mental health or genetic information) could result in inadvertent breaches of confidentiality by requiring different standards for the handling of this information.

**HEALTH CARE AND THE INFORMATION AGE**

The development of the national information infrastructure (NII) is a key component of health care reform. Efforts to reform this country's health care delivery system will rely heavily on administrative simplification and computerization of health information to control costs, improve quality of care, and increase efficiency. The Institute of Medicine (IOM) report, The Computer- Based Patient Record: An Essential Technology for Health Care, recommended the adoption of computer-based patient records by the year 2000 and the formation of a nationwide health information network. However, as that report noted, there are states that require medical records to be written and signed. In order to facilitate the development of a national health information infrastructure, it is imperative that health information can be created, authenticated, and retained in electronic form.

Currently, the expanding use of information technology in health care raises questions about the ability of health-related organizations to ensure the security of health information and to protect the privacy of their patients. In March 1997, the Computer Science and Telecommunications Board of the National Research Council released a report, For the Record: Protecting Electronic Health Information. The report recommends that all organizations that handle individually identifiable health information adopt a set of technical and organizational policies, practices, and procedures to protect such information. It was noted that "adoption of these practices should help organizations meet the standards to be promulgated by the Secretary of Health and Human Services in

connection with the requirements of the Health Insurance Portability and Accountability Act”.

The report also outlines possible legislative options for addressing systemic concerns:

- Legislation to restrict access to patient-identifiable health information based on intended use
- Legislation to prohibit specific practices of concern to patients
- Legislation to establish information rights for patients
- Legislation to enable a health privacy ombudsman to take legal action

The report notes that passage of the Health Insurance Portability and Accountability Act is “a first step toward giving patients greater ability to protect their health information but efforts to extend the fair information practices requirements of the Privacy Act of 1974 to the private sector would empower the consumer population with enforceable rights and create a powerful force for protecting the privacy and security of sensitive information”.

To meet today's information requirements, the nation must move towards a health information infrastructure that will support computer-based patient record systems that capture clinical information, integrate it with clinical support and knowledge bases, and make it available for legitimate users.

Because health information remains largely uncomputerized and unintegrated, patient information is often inaccessible at the time health care decisions are made. Highly trained health care professionals spend valuable time looking for records, contacting each other to obtain basic information, and struggling to decipher handwritten entries or repeating tests because previous results could not be found or obtained quickly enough. National studies have estimated that health care providers spend on average approximately 40 percent of their time on paperwork. External users of health information, such as payers, researchers, governmental agencies, and others must depend on a limited set of data that often is not transmitted electronically, or sort through volumes of records for key information about an encounter.

A number of benefits can be achieved through widespread use of computer-based patient record systems. Health care providers would have more complete information about the patient instantly and easily. Care would be improved through the ability to access knowledge databases and online expert systems. Information systems would reduce the enormous paperwork burden that providers currently experience. Aggregated data from these medical records will enable better research.

One of the major prerequisites to the appropriate implementation of the computer-based patient record is the need for federal preemptive legislation to protect the confidentiality of health information. In order to move health care delivery systems into the 21st century, AHIMA believes that the nation cannot wait any longer to enact federal

preemptive confidentiality legislation. It is critical, and arguably, the most important aspect of any health care reform effort.

#### **AHIMA'S POSITION**

In February 1993, in order to address the need for federal legislation, AHIMA drafted model legislative language that outlined a code of fair information practices. This language was published in the OTA report, Protecting Privacy in Computerized Medical Information, as a model code and was used in the drafting of the "Fair Health Information Practices Act" (HR 52).

There are a number of key provisions in AHIMA's model language that we believe are essential elements of any legislation to govern the collection, use, and disclosure of health care records. These include:

- **Disclosure** -- No person other than the patient or the patient's representative may disclose health care information to any other person without the patient's authorization, except as authorized.

No person may disclose health care information except in accordance with the terms of the patient's authorization.

The provisions apply both to disclosures of health care information and to redisclosures of health care information by a person to whom health care information is disclosed.

- **Record of Disclosure** -- Each person maintaining health care information shall maintain a record of all external disclosures of health care information made by such person concerning each patient, and such record shall become part of the health care information concerning each patient. The record of each disclosure shall include the name, address and institutional affiliation, if any, of the person to whom the health care information is disclosed, the date and purpose of the disclosure and, to the extent practicable, a description of the information disclosed.
  
- **Patient's Authorization; Requirements for Validity** -- To be valid, a patient's authorization must:
  1. Identify the patient;
  2. Generally describe the health care information to be disclosed;
  3. Identify the person to whom the health care information is to be disclosed;
  4. Describe the purpose of this disclosure;
  5. Limit the length of time the patient's authorization will remain valid;
  6. Be given by one of the following means --
    - a) In writing, dated, and signed by the patient or the patient's

representative; or

b) In electronic form, dated and authenticated by the patient or the patient's representative using a unique identifier.

The AHIMA model also includes the following principles of fair information practices:

- **Patient's right to know** -- The patient or the patient's representative has the right to know that health care information concerning the patient is maintained by any person and to know for what purpose the health care information is used.
- **Restrictions on collection** -- Health care information concerning a patient must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected.
- **Collection and use only for lawful purpose** -- Health care information must be collected and used only for a necessary and lawful purpose.
- **Notification to patient** -- Each person maintaining health care information must prepare a formal, written statement of the fair information practices observed by such person. Each patient who provides health care information directly to a person maintaining health care information should receive a copy

of the statement of a person's fair information practices and should receive an explanation of such fair information practices upon request.

- **Restriction on use for other purposes** -- Health care information may not be used for any purpose beyond the purpose for which the health care information is collected, except as otherwise provided.
- **Right to access** -- The patient or the patient's representative may have access to health care information concerning the patient, has the right to have a copy of such health care information made after payment of a reasonable charge, and, further, has the right to have a notation made with or in such health care information of any amendment or correction of such health care information requested by the patient or patient representative.
- **Required safeguards** -- Any person maintaining, using or disseminating health care information shall implement reasonable safeguards for the security of the health care information and its storage, processing, and transmission, whether in electronic or other form.
- **Additional protections** -- Methods to ensure the accuracy, reliability, relevance, completeness and timeliness of the health care information should be instituted. If advisable, additional safeguards for highly sensitive health care information should be provided. The AHIMA model language also contains

provisions for civil and criminal penalties to protect against unauthorized use or disclosure.

AHIMA is pleased that the "Fair Health Information Practices Act" contains many of the provisions based on the code of fair information practices contained in AHIMA's model language. We strongly support the concept that individuals have the right to know who maintains health information and for what purpose the information is used. Many Americans have never seen their personal health records and are unaware of the information contained in them.

Section 101, Inspection of Protected Health Information, and Section 102, Amendment of Protected Health Information, will provide all individuals with the right to access their personal health information. These provisions also provide for the right of individuals to access their health information to amend errors if they do exist.

We note, however, some concerns about sections 101 and 102 regarding inspection copying and correction of information. These sections require health information trustees who a health benefit plan sponsors, health care providers, health oversight agencies, or public health authorities to permit individuals to inspect and copy health information maintained by the trustee. These sections also require that trustees correct or amend protected health information upon request or take certain actions if they refuse to make requested corrections or amendments. Because the medical record is the legal record of the physician or health care facility and is important to continuous treatment of the patient

we urge that a provision be added to exempt from sections 101 and 102 those health information trustees who do not provide care to individuals and are not responsible for the creation and maintenance of health information.

AHIMA strongly believes that individuals have the right to know who maintains their health information and for what purpose the information is used. Health care information is extremely personal and sensitive information, that if improperly used or released, may cause significant harm to an individual's ability to obtain employment, education, insurance, credit, and other necessities. Health information concerning an individual must be collected only to the extent necessary to carry out the legitimate purpose for which the information is collected. There must be limitations on the use and disclosure of individually identifiable health information. The bill addresses these issues in Subtitle B, Use and Disclosure of Protected Health Information. Health information is used for a variety of legitimate purposes, including patient care, quality assurance, education, research, public health, and legal and financial interests. Regardless of the use or users, individuals must be assured that the information they share with health care providers will remain confidential.

We are pleased to note that the language is clear on the distinction between internal access to and use of health information by health information trustees and external disclosure of health information. It is important that information flows within integrated health delivery systems and that no barriers are placed on providers who are trying to provide quality care to patients. There are many appropriate uses of health information

within an organization and it is important to allow persons not involved in direct patient care to have access to carry out their responsibilities.

AHIMA strongly supports the need for mechanisms that will allow individuals to enforce their rights. We are pleased to note that Subtitle E, Enforcements, addresses civil and criminal sanctions.

#### **SUMMARY**

The movement of patients and their health care information across state lines, access to and exchange of health care information from automated data banks and networks, and the emergence of multi-state providers and payors creates a compelling need for federal law governing the use and disclosure of health care information.

AHIMA believes that it is critical for federal preemptive legislation to be enacted. AHIMA extends its thanks to the Subcommittee for holding this important hearing. We hope that this testimony will prove helpful to the Subcommittee. In addition to the points we have made here, we have additional technical comments which we would be pleased to offer as you continue work on the provisions of the "Fair Health Information Practices Act".

Thank you for the opportunity to present our views. AHIMA looks forward to working with this Subcommittee and the Congress to enact legislation to protect an

individual's right to privacy and to ensure the confidentiality of individually identifiable health information.

Mr. HORN. Well, we appreciate that very thorough statement, and we will take you and others up on that because this is a continuing dialog. We don't claim to know it all up here. That is why we have hearings, and in hearings we try to bring out what are the similarities and differences.

Let's start with you, Ms. Goldman. From what you heard from two of your colleagues, where do you differ from them?

Ms. GOLDMAN. Well, I wouldn't want to pass up the opportunity to find differences with my colleagues, but in truth, I am extremely heartened by how much agreement we all have. It has been the true history of this issue that all of us at this table, representing the various organizations, have worked closely together and believe that we must have health privacy legislation. On the broad principles, it seems to me that we have very strong agreement and we have worked together over the years to try to fashion some kind of a consensus. I am not sure there is vast disagreement or even significant disagreement at this time.

Mr. HORN. So you are OK on the principles, but it is the nitty-gritty that sometimes brings the Congress to a halt. Does any of the nitty-gritty bother you?

Ms. GOLDMAN. There are probably some vast differences among folks who are not at this table, but I think if it were left to the three of us we could probably come up with something—

Mr. HORN. The next panel is going to join us, and we asked you all to stay here to get a dialog between the six of you; but I thought we would do some of it first so we could have a few things that are strictly in your testimony.

Ms. GOLDMAN. I think what is remarkable about this issue is, you have organizations such as the American Medical Association and the American Civil Liberties Union and the Center for Democracy and Technology. You have such a broad range of groups who are involved in various aspects of the health care system who realize, from a very first-hand knowledge, how important it is to have enforceable rules.

Mr. HORN. Dr. Palmisano, how about the AMA? Where do you agree and where do you disagree about what you have heard by the fine witnesses on either side of you?

Dr. PALMISANO. Well, I would second what we just heard. I think we are in basic agreement.

What I would like to emphasize is, I think the patient rights need to be superior to the Government's need to know or some other third parties need to know and we should follow established procedure. Certainly nothing less than probable cause to get into the medical record, and we must always protect that right; and we think very strongly the code of medical ethics is something that we rely on very heavily and it states very clearly that the patients' rights are primary. I believe our society is a society that has decided we go to the patient first. It is a philosophical base where the patient has the right to make a decision, even if it is the wrong decision, as opposed to teleological society, where we do what we think is right for the patient and the patients' desires become secondary. So I think we are all in sync on these issues.

We are concerned about some aspects in the bill. We are concerned about the definition of "health oversight agency" seems

overly broad. We understand there may be some agencies that look at this with proper credentials, but maybe there are agencies like XYZ that is a for-profit corporation that gets a hold of this information.

We are very concerned about anything that would allow people who don't have the knowledge and the ethical base to protect the patients' rights having control of these records. We are concerned about anything that would link to Social Security numbers, where someone could get in. We are concerned about crackers or perhaps hackers getting in this information, if it is a clearinghouse. We see the Central Intelligence Agency, recently in the news, reports where some hacker—cracker, I am not sure what the right term is.

Mr. HORN. You can use both, if you want.

Dr. PALMISANO. The evil people that get in without our permission—and they said the Central Stupidity Agency; and we think that is one of our most secure and secret agencies, if people can get through their fire walls, that is what bothers us. And once people know this information is available in electronic form on a central data base, we think there will be great incentives. Right now they are just people doing it to show they can, quote, "beat the system," perhaps, but there will be people selling this information.

So we are very concerned. We appreciate the opportunity, and I will be happy to deal with any specific questions. Thank you.

Mr. HORN. Dr. Johns, what is your feeling based on the testimony your two colleagues have given? Any agreement, any disagreement?

Ms. JOHNS. Very much agreement, Mr. Chairman, and I think as a result of the ongoing policy debate, which occurred over the past several years, we have come as a group to a consensus about the need for this type of Federal confidentiality legislation.

Mr. HORN. Let me ask a few questions before we go to the next panel.

Ms. Goldman, some patients may be willing to volunteer information about themselves or even waive their right of record confidentiality if the waiver is incorporated into an offer from a health care marketer to provide free samples or coupons that might fit the patients' needs. Is a purpose of H.R. 52 to discourage that activity, and should it or shouldn't it?

Ms. GOLDMAN. I think you raise one of the critical issues in privacy legislation, which is consent. It's usually the cornerstone of any piece of privacy legislation, as you may not use the information in an unrelated way, without the individual's consent.

And as we heard from other testimony, consent is a big term, but it doesn't mean anything if it is not voluntary, if it is not informed. It is not meaningful if it doesn't have those qualities to it. And I think the way to ensure consent is meaningful and informed and voluntary is to make sure that obtaining that consent is not a condition of receiving certain benefits and services.

I should be able to go to a doctor and say, I do not want you to release this information to a researcher, or I don't want this information to be released to another doctor without my knowledge; and I should still be able to receive treatment even if, as Dr. Palmisano said, it may not be in the patient's best medical interest. That is

a decision he or she should be able to make without suffering the consequence of not getting care.

Most people who sign the broad waivers, when they go to get health care, the broad waivers that say this information may be released for any purpose to anybody under any circumstances—and I have signed many of them recently since I had surgery on my foot a few months ago, and you sign them because you know that it is not a choice. These are not real choices people are making; and what we should do is build in a way of removing the authorization process or consent process from the receiving of certain benefits and services, and then I think we will see.

In fact, the Video Privacy Act, which I keep raising as an example of what we can do when there is consensus in the Congress, says you may not disclose without permission and you may not request that authorization as a condition of giving someone a video, so can't we do the same thing here?

Mr. HORN. Any comments either of you have on that question?

Dr. PALMISANO. Mr. Chairman, I would just agree with that. In my personal practice over the years, it is not uncommon to get a request about treatment I have given to a patient that may be unrelated to the treatment I just gave, and they make a photocopy of this blanket consent. It is our policy and has been ever since I started medical practice 26 or 27 years ago to always call the patient, and if the patient is not immediately available, I have my staff continue to try and say this information they want is really not related.

I want you to know what is in your medical record. If you have questions, you are welcome to come by and look at it, but you did confide to me some information that has a bearing on why you might have this ulcer, because of the stress, the family problems at home, and I don't believe that is anybody's business, unless you want it to be somebody's business.

So patients feel rather intimidated. They are afraid they are going to lose their insurance, and now in this era of managed care, they could really have additional pressure put on them. They feel rather intimidated, so I think what we have advocated today and what you all are very wisely looking into is in the patients' best interest.

Thank you.

Mr. HORN. Dr. Johns, any comments?

Ms. JOHNS. We fully agree with the statements that have been previously stated.

Mr. HORN. OK. Let's move to the disclosure to spouses. I understand physicians are often faced with difficult choices in sharing that information about the condition and care of a patient with spouses and family members. Assuming a patient had not previously authorized disclosure nor prohibited it, how would H.R. 52 affect the ability of a health care provider, such as physician, to share information with a spouse, and what is your feeling on that, any one of the three of you?

Ms. GOLDMAN. Spouses are not necessarily treated differently from others who are requesting information. The one area where there may be slightly different treatment is called the next-of-kin provision, which allows a doctor to disclose to the next-of-kin,

which could be a spouse, it could be a cousin, it could be someone with whom the individual has a significant relationship. It allows the physician to disclose to that person, for instance, after surgery, unless the individual has objected and said, I don't want you to talk to my spouse about my condition or about the results of my surgery, and so the spouse still has that option.

I assume you would be able to talk with more knowledge about how it works in the real world, but there is usually a more comfortable relationship there unless the individuals suggest they don't want that shared. I think H.R. 52 deals with that pretty well.

Dr. PALMISANO. Well, I think this is a balancing act and something we face all the time. If I am examining a patient—let's say, a woman and she requires an operation—and she says, "please allow my husband to come into the room during this discussion," then I know that she wants her husband to know everything and would want him to know everything in the immediate post-operative period, perhaps, and so on, so there is no problem.

But if someone comes to me, man or woman, and I treat the individual, and someone calls up from another State and says, "Hi, I am the spouse," or whatever, I don't give that information out. There has to be identification, and I have to find out from the patient, "Do you want me to release this information?" Sometimes we find people are judicially separated, for instance; we don't really know they are judicially separated, and they are in the midst of a battle that would affect the division of their assets and so on, so I always go back to the patient.

Basically, our reading of the next-of-kin provision on page 35 is that they would be basically granted the right to give that information, unless the patient objected to that; and that is a balancing act that needs to be decided. So I don't know what is the correct answer to that.

We always go back to the patient, and if the patient is unconscious, comes in from an automobile accident, for instance, in our State in Louisiana, there are provisions that state you can release the information to a next-of-kin. If someone is in a terminal, irreversible coma and hasn't made out a living will, we have a provision in many of the State laws that says the next-of-kin, if not judicially separated, is the individual that can make the decision whether or not to continue life-sustaining treatments if imminent death is there.

Mr. HORN. Suppose it is a transmittable disease that could lead to death; does the spouse have a right to know?

Dr. PALMISANO. Well, of course that is under State law. In almost every State there is a reporting requirement. Some States require you name the individual; other States, they say you give the information immediately to the health officer, and if it looks like it could be something that could affect, for instance, someone with tuberculosis, with a productive cough that has the actual bacteria that causes tuberculosis, if that is being spread around, they need to know the name of the individual and so on. Our medical ethics say that you release the information if someone could do grievous harm to someone else.

So you have to then make a decision. You advise the individual that it is best for you to disclose this, if you are talking about a

sexually transmitted disease, such as AIDS, which usually is considered fatal, but now we have some drugs that may change our perspective on that. Then if the individual says, "no, I am going to continue to do this," I think the physician has an ethical obligation to take the next step and decide whether or not you will transmit the information.

First of all, you have to do it to the health officer, usually, in your State and call the individual. It is one of those ethical dilemmas that the physician needs to make sure that he or she really has all the facts. If someone had a plague that was transmittable by just exhaling and so on, we would need to isolate that individual; and if the individual says, I am out of here, it would be the physician's obligation to notify not only the next-of-kin, but the health authorities, so we wouldn't have a plague throughout the Nation.

Mr. HORN. Dr. Johns, any comments?

Ms. JOHNS. No, basically the comments and the sections within H.R. 52 that have been already been elaborated on, we feel comfortable with.

Mr. HORN. Let me move to another area then on correcting patient records. Dr. Palmisano, H.R. 52, subtitle (a) permits patients to inspect their health care records to make corrections. With what frequency do patients currently ask you, or other doctors, to see their records and attempt to make corrections? And to what degree does that even occur?

Dr. PALMISANO. Mr. Chairman, that is a rarity. It is not unusual for people to request a copy of the records because they may be moving to another State, but it is a rarity for someone to come in and say—in fact, in 26 years of private practice, I have never had anybody come in and say they wanted to change the record. They see me do the record for the office visit right in the office, because after I do the history and physical examination, I usually start writing in front of the patient and ask if they have additional questions, and I tell them of their lab reports and so on, and offer a copy to them.

So I have had people ask for copies of the records, and we give them that information. And in the field I am in, in surgery, it would be rare for me to have something in there that might affect the health of the individual, their mental health, such as psychiatrists might have. There might be information that if the patient got that information immediately—and Dr. Hoge can address that better—but the patient may get even more depressed and commit suicide. So it is a rarity in actual practice, but there is no hesitation on our part for the patient to get a copy of the record.

We believe that the record is the record of the physician, and certainly we wouldn't want to give the original record and have them start changing, and mark out things and so on. But if they want to give me additional information—it is not uncommon, they would say, Doctor, I would like this medicine listed that I have here put in my record; I would say, certainly, and we will photocopy it and give them a copy back, and we will keep the copy, the original or the copy, whatever they prefer, in the record.

It is a rarity that someone would want to take my records and change what is in my record.

Mr. HORN. What State do you practice in?

Dr. PALMISANO. I am in the State of Louisiana.

Mr. HORN. Does Louisiana have a law that relates to this type of situation, or do you follow an AMA protocol, or how do doctors sort of make up their minds how to handle the questions, rare though the question might be?

Dr. PALMISANO. Specifically, we follow the AMA ethical guidelines throughout the Nation, the people who are members of the AMA and many physicians who are not members also follow, whether or not they have sent their dues in. This seems to be the bible of what is the right thing to do.

In Louisiana, on that specific issue—I don't recall if there is any—well, I take that back. We have a statute, in fact, patients have the right to get their record at any time. They can come in and ask for the record, and the record would be given to the patient. If an attorney sends a subpoena in Louisiana—and this law changes every year, but now it will change every other year, because Louisiana now will have a fiscal session 1 year and everything else the other year. But between the medical association, the trial lawyers and everybody else, there is a battle on how to get the record. What we have is a very rigid way of getting the medical record. A patient can come, request the record, sign for the record and get a copy of the record.

If an attorney wants the record through subpoena, that attorney is obligated to send a notification to the patient, if it is an adverse attorney, to the patient or the patient's attorney; and after 10 days to 15 days—it changes from year to year—if there is no protest at the court level, then the physician is allowed to give the record out. But you cannot give the record out until that number of days have passed and you also have this notification; it is an affidavit that the attorney must submit.

So we are very cautious about who can get the record.

Mr. HORN. Do you, in your own practice, or do doctors you know, have they ever refused to grant a patient's request to access to the record; and if so, what is the policy of the AMA on that?

Dr. PALMISANO. No, I don't personally know anyone who has refused to grant access of the patients to the record. I have seen situations where a patient said, don't give that record; and a subpoena came for the record, and the doctor says, what am I supposed to do; and they will usually call the legal counsel or the medical society or their professional liability carrier, and they all get together and try to work something out. They usually end up going to the judge and trying to explain the situation.

But there is no problem in giving that information, and it is the policy of the AMA that the patient has a right to inspect his or her records, unless there is some overriding reason that might, as I said, in a psychiatric situation—my counsel here just pointed out that the patient has access unless in the professional judgment of the medical doctor it would harm the patient—then it goes to some designee, for instance. And this usually occurs in a psychiatric situation, and it is not only in our policy, but it is also in our code of medical ethics book and the patient has a right to that information.

We deal with informed consent, Mr. Chairman, all the time, and it is a very strict law of informed consent that has evolved throughout the Nation and especially in Louisiana.

Mr. HORN. If we use an analogy to an audit report of an organization, often when an auditor makes a statement—let's say it is a Government auditor—the agency would be given the right to respond to that statement; but both items would remain in the record, in other words, the audit initiation and the agency response.

Now, in terms of using medical information—and we talk about the patient's right to correct the record—would that mean we simply add, as you suggested earlier, another sheet of paper to the record, that this is the patient's view of this record, or would there have to be integration in what is presumably your record on the patient?

Dr. PALMISANO. Well, the original record is never changed unless there is an error in the record. For instance, if the physician wrote down the patient was on XYZ medication and, in reality, the physician did not hear that correctly and the patient says, gee, I looked at my record and I am not on that medication, then we don't want to go back and alter the record incorrectly. We want to do it in the approved methodology and make a new note, put an asterisk or some note saying, this is an error up above, put a line through it, date it, initial it; and then go down to the next area for writing and say, this area was corrected, the patient brought it to my attention, the patient is on this medication and not what we wrote. You would then, just move on and that would be the way to correct it.

Now, on the other hand, if what the physician found was absolutely correct, such as the physician did an abdominal palpation and found a pulsating mass or suspected it to be an abdominal aneurysm, that was the physician's impression, based on the history and the physical examination at that time, the symptoms in the physical examination. So if the patient came in and said, "I want that changed, I don't want that on my record because I am going to such and such—I am applying for new insurance," the physician could not ethically or medically or legally do that. That would be wrong.

And if the patient wanted to insert that in there, I personally would have no objection; I don't think it would be in the patient's best interest, but I would put it in the record and say, I will make an attachment page. If the patient came in and wanted the record changed, I don't believe that is the appropriate thing to do.

Here is the patient's statement and put it in there.

Mr. HORN. Any comments on this aspect of record changing, correction or revision?

Ms. JOHNS. The general practice, just as Dr. Palmisano has stated, where there is an error in the record, it is corrected by putting a line through the error, indicating that there is an error, and writing a correct entry for that; and the issue of the amendment to the record is common practice. Good information practice is to include the amendment to the record, if the patient and the health care provider are in disagreement.

Mr. HORN. Is that practice sort of the basic code of your organization, and is that actually carried out in most State laws with which you are familiar?

Ms. JOHNS. It is a practice. Our best practice—our association puts out practice briefs, and that procedure that I have just stated is included as best practice. Whether or not it is carried out in each State would be another issue, but as far as our credentialed, certified people, this is what we would expect.

Mr. HORN. Did you have a comment on that?

Ms. GOLDMAN. Just a small comment.

While I appreciate what the code of ethics is and how, in particular, Dr. Palmisano operates in his practice, my recent experience has been a little disconcerting.

I was in a surgeon's office recently where the patient in front of me requested a copy of her medical record and she said, "May I get a copy of my medical records, please?" And the person behind the desk said, "To whom should we send the record?" And she said, "I would like a copy for myself." And she said, "I can't release the record to you, but if you would like to tell us who you would like us to send them to, we will make sure the doctor gets the record."

She went through a huge struggle, and I then couldn't help myself and suggested there was a law in the District of Columbia that required that she get a copy of her record. And the nurse was furious and said, "That is not our policy in this office, we don't release records to the patients;" and my understanding, in talking to the nurse later on and the doctor—who, by the way, I chose for his surgical ability and not his adherence to privacy principles—I was really surprised to find that at least in the District, there is something that is considered to be common practice which is not to give the record directly to the individual, even though there is a law that requires it.

So I think that, at least in my little experience, there may be a real disjuncture between what the code of ethics is and how people practice.

Mr. HORN. On, quote, the record, unquote, what about a xerox of the record? Are they worried about the complete loss of the record? That is a legitimate worry for a doctor.

Ms. GOLDMAN. I assume so.

Mr. HORN. I assume they would make a xerox to send it even to another doctor, rather than lose that record. I would never release a record like that.

Ms. GOLDMAN. The issue, at least in the circumstances I am giving, is not so much whether it was xeroxed or not xeroxed, but that the practice, the policy of that office was not to release directly to the patient.

Mr. HORN. I understand that; and I think the law is right and the doctor's office was wrong, that the patient ought to have a right to know, even if they can't translate the doctor's handwriting and even if they don't know what some of the words mean.

Let me ask you, Dr. Johns, about audit tracing. Many information technology systems can incorporate these records, handling audit trails that maintain a log of each instance—when each individual is looking at an electronic file. We have that argument in Government as to who had access to these files. This makes it pos-

sible to generate a list of each time and each individual who has looked at a patient's electronic record.

How prevalent are such tracing procedures in existing health care information systems? Do they have that type of situation?

Ms. JOHNS. With electronic information systems, there are usually provisions or functions for audit trails, and audit trails are used in various ways. It is not that they are included with the patient's medical record, but they are used as one mechanism in a total security policy; and I think that is important, to recognize that audit trails or tracings are one avenue by which you can protect or identify breaches of confidentiality or at least identify breaches of access into the record.

A total security policy should include good policies, good procedures, very good employee education and training, in addition to being able to select various types of technical types of mechanisms that can protect information in an electronic environment.

Mr. HORN. I think one thing that worries a lot of us—and I remember the testimony very clearly when Mr. Condit chaired the subcommittee under the Democratic Congress, one of our colleagues from New York had had her records stolen, and entered into her political campaign. In other words, her records were used against her.

That was a very serious situation, and I think all of us worry about the person who has access to those records in a doctor's office, in a hospital, in an insurance company, whatever the case may be. You could have a disgruntled employee who decides to take copies of the records of the mayor of the city and the biggest developer in town. They would be subjected to blackmail are subjected to revelation of an embarrassing situation by sending the information to the local newspaper.

Now, what kind of audit system do we have in one's office to say, who has access to these files? As I go into offices, what I see are rows and rows of paper folders. And often when I go in, there is nobody behind the desk; if it is the noon hour or whatever, somebody could walk through and say, that is an interesting folder, I think I heard her on TV the other night. So what do we do about that?

Ms. JOHNS. In relationship to access to paper records, normal practice is that when records are released, there is a log that is kept as to who has requested that information and for what purpose. This would be occurring in hospital medical records departments.

In regards to the instance that you were giving, as far as like an employee who might want to access records, if they felt they were going to be terminated, another good practice is that individuals who are going to be terminated, their access rights, in addition to audit trails, need to be terminated prior to them being informed of their termination, or at the same time, so that you have dual types of counterbalances, as far as protecting that information.

Audit trails, too, can have intelligence built into them so that flags are set as to identifying potentially suspicious types of activity. For instance, if an employee of the health care facility was being treated in the hospital, any accesses to that record would be monitored and flagged, if it would be a health care provider that

would be looking at the record who didn't have the direct patient contact relationship, or if it would be an employee within the institution someplace, where they should not have access.

So I think an important consideration with audit trails, as well, or tracings, is that there is some mechanism by which potentially suspicious activities can be identified.

Mr. HORN. Should hospitals, insurers, doctors, and other health care providers be required to incorporate such tracking procedures in all the information systems?

Ms. JOHNS. I think that is an issue you have to look at in context, and again, as I mentioned, audit trails are only one technical aspect of a security program. You have other aspects, such as passwords, access levels, audit trails, certainly, and policies and procedures, as well as employee education and training.

So, I think you really need to look at the specific application—how large the institution is, for instance—in a smaller physician's office practice, the need for audit trails when you have three people working in an office may really not make much sense, as opposed to an institution where you have 5,000 individuals working and more people who have access, and clearly all of them would not be involved with the direct patient care.

So I think it needs to be done, all of the guidelines need to be presented, and then a mechanism of procedure for a whole security program needs to be developed. I think that is going to be varied from institution to institution.

Mr. HORN. One last question before we move to the next panel concerns administrative simplification.

One of the objectives of the Kassebaum-Kennedy bill, which was enacted into law, as I mentioned in my opening statement, was to foster administrative simplification. This includes creating common definitions for data elements and coding practices.

Three weeks ago, this subcommittee heard testimony on the medical transaction system of the Medicare operation, and the Department of Health and Human Services and their efforts to develop a common provider identification number. Are we making progress toward streamlining health care administration practices and what barriers continue to exist? What do you see happening in that area, Dr. Johns?

Ms. JOHNS. As far as barriers in electronic patient records?

Mr. HORN. Yes, and just how far are we from it.

Are we getting into standardization based on software of a particular vendor, or is that software related to the best practices of your organization, the AMA and others?

Ms. JOHNS. I think one very large barrier—and it has been cited by other reports—the Institutes of Medicine and their computer-based patient record report even back in 1991 cited one of the biggest barriers is lack of standard, and a barrier we certainly are experiencing is the barrier in regards to confidentiality and having Federal legislation in regards to a standard, uniform practice. And so, without some standard, uniform practice, it makes it very difficult to either transfer information—we have problems with standards in vocabularies which, of course, agencies or groups like the National Library of Medicine are certainly working on, other groups like HL-7 and ASTM standard organizations are working

on. I think that, because HIPA requires the Secretary of Health and Human Services to adopt standards for national providers, identification, payers, and patients by February 1998.

We feel that this is a very good first step in helping us get the standards that we need to build a national information infrastructure, and I believe the NCVHS is currently holding hearings on these issues, and additional information will be available later this year, which certainly we will comment on at that time.

Mr. HORN. Well, we thank you for your comments on this series of questions.

We are now going to ask panel III to come forward and sit with you. You can relax for a while and then we have some comments, questions for both panels II and III. So if Dr. Gabriel, Drs. Andrews and Hoge will come forward, we will appreciate it. If the new witnesses will stand and raise their right hands.

[Witnesses sworn.]

Mr. HORN. All three witnesses have affirmed.

Let's just go down the line, the way the agenda is.

Dr. Sherine Gabriel, Department of Health Services Research, Mayo Clinic, representing the Healthcare Leadership Council, is first.

**STATEMENTS OF DR. SHERINE GABRIEL, DEPARTMENT OF HEALTH SERVICES RESEARCH, MAYO CLINIC, REPRESENTING THE HEALTHCARE LEADERSHIP COUNCIL; DR. ELIZABETH ANDREWS, GLAXO WELLCOME INC., REPRESENTING THE PHARMACEUTICAL RESEARCH AND MANUFACTURERS ASSOCIATION; AND DR. STEVEN KENNY HOGE, CHAIR, COUNCIL ON PSYCHIATRY AND LAW OF THE AMERICAN PSYCHIATRIC ASSOCIATION**

Dr. GABRIEL. Mr. Chairman, members of the committee, I am Dr. Sherine Gabriel, a physician and researcher at the Mayo Clinic. Thank you for the opportunity to testify before you today regarding the issue of medical records confidentiality.

I am here this morning, as you just heard, on behalf of the Healthcare Leadership Council. My testimony, however, will reflect my own perspectives as a health care researcher. I will address two fundamental questions: What is the importance of medical records-based research to the public, and what is the impact of legislation restricting access to medical records on such research?

I am privileged to work at a world-renowned medical institution. Mayo Clinic's international reputation is a center of excellence in medicine, which grew out of the commitment of our founders, Drs. Will and Charlie Mayo, to integrate medical research and education with clinical practice.

The Mayo brothers perceived a duty to use the information from medical records to answer important public health questions, and in 1907, pioneered the concept of the unit medical record, where medical data on each patient is stored in one self-contained packet and kept in perpetuity. This led to the formation of the Rochester Epidemiology Project, the unique national research resource which has been funded by the National Institutes of Health for over three decades. It has resulted in approximately 1,000 scientific publications, analyzing thousands of diseases and medical conditions, and

was ranked in the top 1 percent of all NIH proposals when it was last reviewed in 1995. The central element of the REP is access to the complete medical records of all residents within a geographically defined population.

Medical records research is vital to maintaining and improving the health of the American public. Virtually every health hazard we know of today and countless medical advances have been identified using information from medical records. For example, if researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late 1970's, the characterization of the AIDS epidemic would have been delayed at a huge cost to the public's health. Similarly, characterization of Lyme disease required collation of information from the medical records of the children who presented with this condition in Lyme, CT.

Other examples include examining the benefits and risks of estrogen treatment, the health risks of smoking, of dietary fats, obesity, certain occupations, studies leading to the development of vaccines for polio and measles, and studies showing the benefits of breast cancer screening. Without medical records research, problems such as the Thalidomide tragedy and the role of prostate specific antigens, the controversial tests for prostate cancer, could not have been resolved to the extent they are.

You may have read in the newspapers last year that an outbreak of flesh-eating strep was identified at Mayo in 1995. Without access to the medical records of patients with these unusual infections, characterization of this syndrome and isolation of this deadly bacterial strain would have been delayed and over 100 school children, which our research showed were the unwitting carriers of this deadly germ in their throats, would have gone untreated.

Let's now turn to the second question: What is the impact of legislation which restricts access to medical records? Such legislation, in my opinion, threatens the very existence of this entire category of medical research. This is because people who do not consent are systematically different in important ways from people who do.

For example, people who don't consent may have had worse outcomes, or they may be less satisfied with their care. Studies which exclude these people would be biased; they would simply give the wrong answer.

Moreover, while research is clear on the point that people who do not consent are systematically different from those who do, the direction and magnitude of those differences are completely unpredictable from study to study. So not only will such research result in the wrong answers, but it will be impossible to determine how wrong they are or in what direction. Thus, the reliability and validity of the findings from such research will be weakened.

Inclusion of all qualifying individuals is the only way to ensure that accurate conclusions are drawn in public health medical records-based research. Of course, such research—and we recognize this—must be done while taking appropriate measures for maintaining patient confidentiality, including careful review and oversight by institutional review boards and strict adherence to procedures restricting access to patients' specific medical information.

In closing, I want to comment briefly on what I believe is an important driving force behind all of this, which is the desire to keep personal medical information between the patient and his or her physician, the old Hippocratic idea. As a physician, a patient and a mother, I understand why this idea is so appealing; however, in a complex health care environment, it is an unattainable ideal.

For example, in an average medical visit, the following individuals and groups must have access to the patient's medical record in order to best serve the patient: the appointment office; the registration desk; all physicians, physician assistants and nurses who provide care for the patients, as well as receptionists and secretaries; medical, nursing and other students and their mentors; all laboratory, EKG, x-ray technicians who perform the necessary tests; infection control officers who regularly survey medical records for reportable diseases; continuous improvements staff who strive to improve our health care processes; members of the marketing department who seek to ensure patient satisfaction; the business office for billing, the legal department, insurers, and third-party payers.

After all of this is taken care of, a qualified nurse researcher, bound by the rules of the IRB and strict patient confidentiality regulations could be abstracting clinical data from the medical record which, after being stripped of patient identifiers, will be combined with similar data from hundreds of other patients to answer a specific public health question. The type of legislation we currently have in Minnesota influences only that nurse's access to the medical record and has no impact on any of the other points of access.

Mr. Chairman, legislation must be carefully crafted, such that it ensures privacy of medical information, a very important goal, and does not hinder medical scientific research, as such interference will put the public's health and well-being at risk for serious harm.

Thank you for your attention.

Mr. HORN. Well, thank you. You have raised some very interesting questions that we are all going to have to grapple with.

[The prepared statement of Dr. Gabriel follows:]

Good morning, Mr. Chairman and Members of the Committee. I am Dr. Sherine Gabriel with the Mayo Clinic. Thank you for the opportunity to testify before you regarding the most important issue of medical records confidentiality. I am here this morning on behalf of the Healthcare Leadership Council (HLC), a Washington, D.C.-based trade association uniquely representative of the broad health care industry. The HLC members include the managed care, hospital, pharmaceutical manufacturer, device manufacturer and professionals in the provider communities.

The HLC members are the innovators in the health care industry, and share a commitment both to the market-driven health care delivery system and to providing high quality health care services to individuals. An important element of our dedication to individual patients is a commitment to ensuring that all identifiable patient health information is kept strictly confidential and used only for purposes of providing health care services, paying for them, and for enhancing the quality of these services.

For more than a year, the HLC members have been engaging in an earnest effort to work with its members and others in the industry to craft workable and meaningful confidentiality protections that provide important assurances to the patient while at the same time allowing health plans, providers and health product manufacturers to use patient health information for purposes that are necessary and appropriate to the provision of high quality health care services.

The key to enacting any workable legislative solution is balance.

In searching for a workable federal legislative solution, the HLC has identified the following principles as necessary to striking the right balance between the patient and the information needs of the health care industry. These basic principles are as follows:

(1) Support federal standards regarding the confidentiality of all patient health information; (2) Treat all identifiable patient health information, including genetic information, the same way to assure the same strong confidentiality protections; (3) Apply standards only to identifiable health information, leaving non-identifiable health information (i.e., coded and encrypted data) available for use in research and for other health-related purposes; (4) Facilitate appropriate uses and sharing of patient health information and recognize that access to information is not harmful, but rather helpful to the patient; and (5) Provide for strong and thorough preemption of state law.

1. **Federal standards.** Federal standards ensuring the confidentiality of patient health information are critical to guaranteeing the uniform, consistent treatment of such information throughout the country. Last year's Health Insurance Portability and Accountability Act (HIPAA) took important steps in the right

direction by requiring that a standardized information transmission and storage system be developed, and that such systems be kept secure. In addition, HIPAA mandates that Congress enact federal confidentiality standards by August of 1999. Failure to do so will trigger Secretarial authority to promulgate regulations guaranteeing such protections.

The time has come for a uniform federal standard, and computer modems that transfer data across state lines and internationally. The HLC supports federal standards regarding disclosure and use of an individual's identifiable health information, for safeguarding the confidentiality of that information, and for establishing an individual's rights to inspect and copy his or her records. A uniform standard is the only way to avoid a dual-regulatory environment. State authority should remain paramount over areas of confidentiality that do not conflict with national uniformity and consistency, such as state reporting requirements for public health and safety dangers.

2. **Treat all identifiable health information in the same manner.** The HLC supports extending strong and consistent confidentiality protections to all personally identifiable patient health information. As such, the HLC is concerned over recent proposals, such as that introduced by Rep. Slaughter (D-NY) (H.R. 306), to treat genetic information separately from other patient health information. As a practical matter, it would be difficult if not impossible for health

plans and providers to treat and secure genetic information differently than other patient health information as almost all health information contains an important genetic component. How then can we elevate certain types of health information to a higher status more deserving of protection than other information? All personally identifiable patient health information should receive the same strong protections against inappropriate disclosure.

Congress recently engaged in a debate over mental health services and concluded that mental health should be treated the same way as physical health services regarding financial limits. Again, given this recent "mental health parity" debate, it is difficult to envision a reason to then treat mental health information differently than other patient health information.

3. **Scope of federal standards should apply to individually identifiable information only.** In its effort to craft federal confidentiality standards, Congress should apply these protections to individually identifiable health information only where there is a legitimate need for confidentiality. The current trend is toward anonymizing information — that is, rendering the information available but leaving the identity of the subject individual unknown — and a more narrow focus on individually identifiable health information would provide an important incentive to encrypt, encode and otherwise anonymize patient health information wherever possible.

The HLC strongly believes that any federal confidentiality standards should provide incentives for health plans, providers, purchasers and other product manufacturers to continue using *non-identifiable* health data to make advancements, cure diseases and study the effects of new treatments. Allowing the use of anonymous health data directly facilitates health research and limiting its use would stifle the phenomenal medical advances being made almost daily in this country. To further ensure the confidentiality of patient health information, however, the HLC strongly supports subjecting any "encryption key" or other such code used to anonymize information to the same strong protections guaranteed to other protected, identifiable health information.

4. **Provide for appropriate health information sharing with confidentiality protections.** Any federal confidentiality standards adopted by Congress must adequately and effectively recognize that most health care services are delivered through some form of integrated delivery system. This modern health care system, which is marked by a team-approach to health care delivery, relies heavily on information sharing and collaboration to ensure high quality services are provided to the patient. As a result, it is crucial that strong patient confidentiality protections allow and facilitate appropriate information sharing to further this goal. Following are several key points explaining the HLC's perspective:

- **An integrated health care delivery system requires more information sharing.** Only in focusing on what are and are not appropriate "uses" of patient health information can we develop confidentiality protections that effectively distinguish between what is helpful and harmful to the patient and to consumers generally. Our health care delivery system is no longer one defined by discrete encounters with a number of different and unrelated physicians and providers. Rather, the current delivery system is distinguished by a growing number of innovative arrangements between and among physicians, health plans, employers, hospitals and researchers. We now have teams of professionals responsible for coordinating the health care services provided to patients. These teams involve multiple individuals, including physicians, nurses, lab technicians, pharmaceutical manufacturers and others. Together, these varied participants are working in the interest of the patient.

As a result of these important improvements in the health care delivery system, the HLC supports establishing strong confidentiality protections consistent with direction of our delivery system. Specifically, the HLC supports allowing the use of patient information for purposes of providing treatment, securing payment, conducting health care research and undertaking quality assurance activities. These activities are all designed to benefit the consumer.

My expertise is uniquely focused on health care research. I am privileged to work at a world renowned medical institution. The Mayo Clinic's world-wide reputation as a center of excellence in Medicine grew out of the commitment of Will and Charlie Mayo to integrate medical research and education with clinical practice. Medical records research is vital to maintaining and improving the health of the American public. In fact, virtually every health hazard that we know of today has been identified using information from medical records. Take AIDS, for example. If researchers had not been allowed to study the medical records of patients with unusual immune deficiency problems in the late 1970's, the characterization of the AIDS epidemic would have been delayed at substantial cost to the public's health. Other examples include studies examining the benefits and risks of estrogen treatment, the health risks of: smoking, dietary fats, obesity, and certain occupations; infectious disease studies which led to the development of vaccines for polio, measles and other infectious diseases; and studies which show the effect of breast cancer screening programs.

You may have read recently that an outbreak of "flesh eating strep" was identified at Mayo in 1996. Without access to the medical records of patients with these unusual infections, characteriation of this syndrome

and isolation of this deadly bacterial strain would have been delayed. And over a hundred school children – which our research showed were the unwitting carriers of this deadly germ in their throats -- would have gone untreated. Every medical advance mentioned here has relied heavily on information from patients' medical records. Without access to this rich source of clinical information, many of these advances simply would not have occurred.

- **You can't expect a surgeon to operate blind.** Legislation must emphasize confidentiality and provide strong disincentives for abuses of information; however, the HLC is concerned over recent proposals that would appear to place the patient in a position of having ultimate veto power over access to information. To put patients, who by and large rely on lay knowledge, in a position of deciding whether to grant access of information to some and not to others ultimately puts them at risk. Again, federal standards should focus on the appropriateness of information disclosure and its use.
  
- **The move toward electronic transmission of information brings forth tremendous benefits for the patient, but also creates fears.** The recently enacted Health Insurance Portability and Accountability Act (HIPAA) will result in numerous standards regarding the security of

electronically transmitted information. The concept of a unified medical record is revolutionary in the benefits that will inure to patients. There will be fewer adverse drug reactions, fewer mistakes made and fewer unintended consequences. Electronic data storage presents a greater opportunity to secure information than in the current system of open file cabinets, etc. At the same time, anything new and unfamiliar can cause trepidation. It is the fear of the unknown. Yet a unified medical record stored electronically actually can keep information more secure than paper copies in files, as mentioned before. Computer records can be safeguarded through encryption, password access and other similar technologies.

- **The HLC is concerned over efforts to use the confidentiality debate to advance other agendas, such as anti-managed care and insurance product pricing issues.** The HLC grows increasingly concerned that the debate over *how* to keep patient health information confidential in the current health care delivery environment is becoming a vehicle for debate regarding the delivery system as a whole. Again, the HLC advocates responsible and appropriate information sharing and use. However, any debate desired about such practices as medical underwriting, utilization review/utilization management and other quality assurance techniques should be held separately and should be dealt with on the basis of their

merits. The HLC cautions Congress against effectively putting an end to such practices through the guise of protecting the confidentiality of patient information.

- **Confidentiality protections are already in place.** Health plans and providers submit to voluntary accreditation, which includes evidence of strong confidentiality protections. For example, the National Committee for Quality Assurance (NCQA) and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) are two accrediting bodies which require health plans and hospitals to have written confidentiality policies and procedures in place, to take action at patient care sites to guard against unauthorized or inadvertent disclosure of confidential information, and to obtain patient consent for information release. In addition, the Federal Privacy Act imposes numerous confidentiality requirements on health plans and providers participating in the Medicare program. Similarly, the Institutional Review Board (IRB) process involving clinical research holds pharmaceutical manufacturers, device manufacturers and other researchers to stringent confidentiality standards.

**5. Strong federal preemption of state law.** The HLC strongly supports effective federal confidentiality protections for consumers as long as the standards include strong and thorough preemption of state law in those areas in which the federal

government has legislated. Without adequate preemption, providers, health plans, purchasers and manufacturers would essentially be subject to 52 different confidentiality laws, which is unworkable and leaves consumers vulnerable under a patchwork of protections.

With these important HLC principles in mind, we are concerned that current legislative proposals, such as that advanced by Rep. Condit (D-CA) (H.R. 52), fail to meet these objectives. Specifically, Rep. Condit's "Fair Health Information Practices Act of 1997," and other similar bills advanced last Congress, fundamentally fails to recognize that most health care services today are delivered in some integrated delivery context. Attached are charts that the HLC commissioned from Multinational Business Services, Inc., which illustrate the enormous complexities involved with compliance, the numerous mandates imposed on health plans, providers and other health professionals, and the important health care services and functions which would be effectively prohibited under H.R. 52. Unfortunately, the complex systems for storage, transmission and disclosure of patient health information created under the Condit approach would not put an end to all inappropriate disclosures of health information. No legislation can guarantee us that result. However, the Condit bill and other similar proposals would severely impede the continued production and provision of high quality health care services. Again, this emphasizes the importance of balanced confidentiality protections.

In a Congress that values the strengths of the private market and that favors removing government mandates and over-regulation, H.R. 52 would move us in the wrong direction.

Any legislative restrictions limiting access to medical records, such as H.R. 52, threaten the very existence of entire categories of medical research. This is because individuals who deny consent are systematically different in important ways from individuals who do consent. For example, individuals who deny consent may have had worse outcomes or they may be less satisfied with their care. Studies describing the outcomes of diseases or the effectiveness or cost-effectiveness of treatments which exclude such individuals would be biased -- they give us the wrong answer. Moreover, while research is clear on the point that individuals who deny consent are systematically different from those who consent, the direction and magnitude of those differences are completely unpredictable from study to study. So not only will such research result in the wrong answers, but it will be impossible to determine how wrong they are or in what way. Thus, the reliability and validity of findings from such research will be suspect and lead to the design of potentially incorrect medical treatments. The inclusion of all qualifying individuals is the only way to assure that accurate conclusions are drawn about the prognosis of disease, the outcomes of therapy or the quality of care.

I understand the underlying motivation for legislation such as H.R. 52 is to keep personal medical information between the patient and his or her physician. As a physician, a patient and a mother, this idea is very attractive. However, in our complex health care environment, it is an unattainable ideal. For example, in an average medical visit the following individuals and groups have access to a patient's complete medical record: the appointment office, the registration desk, all physicians, physician assistants, and nurses who provide care for the patient as well as their receptionists and secretaries, all laboratory, EKG, and x-ray technicians who perform the necessary tests, infection control officers who regularly survey medical records for reportable diseases, continuous improvement staff who strike to improve out health care processes, members of the marketing department who seek to ensure patient satisfaction, the business office for billing, the legal department, and insurers and other third-party payers. After all this is done, a qualified nurse researcher bound by rules of an Institutional Review Board (IRB) and strict patient confidentiality regulations could be abstracting clinical data from the medical record which, after being stripped of patient identifiers, will be combined with similar data from hundreds of other patients to answer a specific public health question. The legislation we are discussing today would particularly influence that nurse's access to the medical record. Mr. Chairman, such legislation does not ensure privacy of personal medical information. Instead, it hinders scientific research and puts the public's health and well being at risk for serious harm.

Again, the Healthcare Leadership Council would like to work together with lawmakers in search of meaningful and balanced federal confidentiality standards. The HLC looks forward to working with you and your staff. I would be pleased to answer any questions the members of this committee may have.

Thank you for your attention.

Mr. HORN. Our next witness is Dr. Elizabeth Andrews—I hope I am pronouncing this right—Glaxo Wellcome Inc., representing the Pharmaceutical Research and Manufacturers Association.

Dr. ANDREWS. Thank you, Mr. Chairman, and thank you for the opportunity to present our information. My name is Elizabeth Andrews and I am director of Worldwide Epidemiology at Glaxo Wellcome. I appear before the committee on behalf of the Pharmaceutical Research and Manufacturers of America, or PhRMA, to discuss our industry's views on data privacy in general and H.R. 52 in particular. I will summarize our full statement, which will be provided for the record.

It is clear that patients deserve to have medical information kept in strictest confidence by those to whom they entrust it. PhRMA companies honor that trust. Patients also deserve answers to their unmet medical needs.

This past year, the research conducted by our companies yielded 53 new FDA-approved medicines, new weapons in the war against 40 diseases, including AIDS, cancer, heart ailments, and mental illness. Our continued progress depends on aggressive, multifaceted research, including basic science that allows us to understand disease processes, practical research and development that enables us to discover and develop drugs to treat disease. Clinical trials that demonstrate project safety and efficacy, epidemiologic research that helps us to know how drugs perform in the real world, identifying and characterizing rare side effects or unsuspected benefits and health services research that leads toward improvements and the quality and cost-effectiveness of patient care. Federal policy must accomplish twin objectives, protecting the privacy of individual patients, while also protecting the continued viability of research that promotes improved health care for all persons.

We believe these objectives can best be met by establishing uniform national requirements for the handling of medical information, defined to include genetic information. PhRMA has three primary suggestions that should be included in Federal requirements, but need specifically to be addressed in H.R. 52.

First, the bill should recognize the process already in place under regulations adopted by FDA and 16 other Federal agencies to protect patient identifiable information used in biomedical research. Second, any new legislation or regulations should preserve researchers' access to the full range of potentially useful information about the incidence, prevalence, and outcomes of illness, as long as individual privacy is properly safeguarded. Only those data sources that directly identify individuals need to be kept confidential.

Third, uniform national requirements should provide effective Federal pre-emption of State statutes. One of the compelling reasons for establishing Federal requirements is to provide a uniform set of rules that can be applied consistently from State to State for research. With respect to clinical trials, the current controls regulating FDA-monitored trials are quite strict.

Through standard operating procedures, companies ensure, under Federal Rules, that personally identifiable information remains secure in the offices of individual health care practitioners who serve as the study investigators. The sponsoring company has access only to the information that needs to report to FDA, to

verify results and to protect patient safety. We are concerned that H.R. 52 does not recognize the existing safeguards, the regulatory processes and oversight mechanisms that exist. The National Institutes of Health and the President's National Bioethics Advisory Commission are already charged with examining the IRB process and will develop recommendations for any improvements that are deemed necessary.

PhRMA is also concerned that H.R. 52 would restrict access to certain data bases if they could be linked by codes to data sources that identify individuals. These data bases contain crypted identifiers and only through the use of a secure and confidential key can specific patients be identified. In some studies, it is necessary to use this key to link to other sources of information about the patients to create a richer more scientifically informed set of data. These type of studies need special precautions to ensure confidentiality of patient information, but these studies are not concerned with the identity of the patient, only with the scientific content, that a patient's information can contribute to a study.

A wide range of health-related data could be affected by the provisions of H.R. 52, from Medicare, Medicaid and private insurance claims data, to State-collected vital and health statistics. Access to these data is important to generate answers to many of today's pressing health issues that cannot be answered through other mechanisms. Analyses of such data have contributed to demonstrating the higher risk of hip fracture in the elderly among those taking psychotropic drugs, quantifying the risks and benefits of hormone replacement therapy, documenting the underuse of beta blockers following heart attacks and the resulting increase in mortality and morbidity.

Under H.R. 52, access to these data bases could be construed to require for each reanalysis of the data, either specific consent of each of the subjects whose medical information is contained in the data base or the approval of a certified IRB. Current regulations exempt such data from IRB review and informed consent requirements. Such requirements are unnecessary and do nothing to protect human research subjects, whose identity is not revealed in such data bases. Instead, we can protect patients' privacy without impeding research, through careful encryption of data, effective security for the key to encrypted data, tight security safeguards whenever confidential information is accessed directly, and guarantees of confidentiality by each individual who obtains confidential information.

In conclusion, the research-based pharmaceutical industry respects the privacy of patients and the confidentiality of information about them. We could not conduct our research if we did not do so. We urge that any changes in Federal confidentiality requirements be drafted with great care to ensure that medical research can continue to yield new remedies and better ways of caring for patients. Thank you.

[The prepared statement of Dr. Andrews follows:]

# Statement



TESTIMONY OF ELIZABETH B. ANDREWS, Ph.D.  
 ON BEHALF OF THE  
 PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA  
 (PhRMA)  
 BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
 INFORMATION AND TECHNOLOGY OF THE GOVERNMENT REFORM  
 AND OVERSIGHT COMMITTEE

June 5, 1997

Thank you for the opportunity to address this Committee on the important issue of data privacy. H.R. 52 is intended to protect the privacy of an individual's medical information by establishing a code of fair information practices for health information. The Pharmaceutical Research and Manufacturers of America (PhRMA) shares the concerns about security of this personal information and has adopted a set of principles that express our views about the need to safeguard this information. These principles are attached to our statement. PhRMA members also understand that medical information on individuals is essential to progress in medical research and is the foundation for the medical breakthroughs that will eliminate or reduce some of the most serious health threats today. The pharmaceutical industry has a vital stake in policies that affect the research on which our entire enterprise depends.

PhRMA represents the nation's leading research-based pharmaceutical and biotechnology companies. PhRMA members discover and develop most of the new medicines used in the United States and around the globe. This past year the industry brought 53 new medicines to market: new weapons against HIV/AIDS, several new anti-cancer drugs, a new anti-depressant and a new anti-psychotic drug, new treatments for chronic diseases such as diabetes, asthma and hypertension, and for many other deadly and debilitating diseases.

Continued progress of this magnitude depends on aggressive, multifaceted research, including:

- Basic science that allows us to understand disease processes,
- Practical R & D that finds the right compound to combat the disease,
- Clinical trials required by law to demonstrate the safety and efficacy of potential products, and

*Pharmaceutical Research and Manufacturers of America*

1100 Fifteenth Street, N.W., Washington, D.C. 20005 (202) 835-3400

- Large-scale epidemiologic research and health services research that helps us know how the drug performs out there in the “real world.” This real-world research detects rare side-effects that may not show up in relatively limited trials, identifies unsuspected benefits a product may have, and evaluates the cost-effectiveness of modern medicines.

All this research is ultimately for and about patients -- and virtually all of us are patients at some point in our lives. Both healthy and sick people participate in pharmaceutical research in many ways. They are certainly entitled to know any risks they are taking. For clinical trials, institutional review boards (IRBs) are set up to make sure patients provide “informed consent” to their participation in research. Patients share sensitive information about themselves when they participate in clinical trials and, for that matter, when they visit a physician or a hospital or submit a claim to a health insurer. They deserve to have this information kept in strictest confidence by those to whom they entrust it.

On the other hand, researchers must have sufficient identifying information about their research subjects in order for the research to proceed in an orderly and accurate manner. They also need demographic and environmental information that can provide clues to the causes of the illness being examined and the effects of the drugs being tested. Clinical and pharmacoepidemiologic research would grind to a halt if researchers were denied access to this information.

Federal policies must accomplish twin objectives: protecting the privacy of individual patients, while also protecting the continued viability of research that promotes improved health care for all patients. We believe these objectives can best be met by establishing uniform national requirements for the handling of medical information, defined to include genetic information.

Within this uniform national framework, clinical trial information should continue to be protected as it is now, by FDA requirements for privacy and informed consent. The rules under which these trials are conducted effectively protect patients’ privacy while permitting essential safety and efficacy evaluation of the trials.

New legislation like H.R. 52 should distinguish carefully between data sources that contain the identity of specific individuals on the one hand; and, on the other hand, data sources that contain patient-level data without patient identifiers or data sources that can be linked to specific patients only through the use of a confidential and secure key which is not available to the researcher. Only those data sources that directly identify individuals need to be

kept confidential. Anonymized or encrypted data sources should be excluded from any new requirements or restrictions applicable to patient-identifiable information. Where confidential keys or links to individual patients are necessary in either clinical trial data or in non-research data bases, such keys or links can and should be maintained securely to prevent inappropriate disclosure.

It is important to stress as well that in establishing uniform national requirements, that these requirements provide effective federal preemption of state statutes. One of the compelling reasons for establishing federal requirements is to provide a uniform set of rules that can be applied consistently from state to state for research. If individual states are permitted to add additional requirements, then the benefits of these uniform rules will be lost and researchers will again be faced with an inconsistent patchwork of requirements.

Concerns about Regulation of Information Handling in IRB-Monitored Clinical Trials

H.R. 52 would impose new federal privacy requirements encompassing clinical trials that could substantially delay research; make it more expensive – perhaps prohibitively expensive; or, in some cases, make the research entirely unfeasible. In our view, patients would be the losers. Pharmaceutical firms already adhere to strict FDA regulations that govern clinical research and ensure the protection of human subjects and the security of the data about those subjects. Additional layers of legislative requirements are simply not necessary and will only slow the progress of this research.

For example, H.R. 52 requires that an IRB, before approving a proposed trial, must judge whether privacy risks to patients of participating in that trial are justified by the potential benefits of the research. The legislation also requires HHS certification of all IRBs according to a process that the Secretary of HHS will specify in regulations. Specifying these requirements in legislation is unnecessary and likely to lead to uncertain interpretation. Moreover, the National Institutes of Health and the President's National Bioethics Advisory Commission are already charged with examining the IRB process and will develop recommendations for any improvements that are deemed necessary. There is no need, and in fact it could be counterproductive, for the Congress to address prematurely IRB requirements in this legislation.

The controls in place over FDA-monitored clinical trials have been carefully designed to promote good scientific and clinical practice while protecting patients' well-being. Existing federal regulations require that a patient receive an explanation of the risks of participating in the trial and of the provisions that have been made to guard confidential information. The trials are

set up so that the actual personal details remain in the offices of the individual health care practitioner. The trial's sponsor normally has access only to the case reports submitted by that practitioner, which contain coded information that allows a check back to the detailed case records at the practitioner's site. PhRMA companies have standard operating procedures wherein the key to the codes is located at the practitioner's site, under tight security.

Existing FDA regulations require personally identifiable information to be retained at the trial site for several years after a drug is approved. There are several reasons records must be kept for a substantial length of time: to make possible audits to demonstrate the integrity of the trial; to enable patients to be contacted should an unsuspected problem be uncovered that could affect their health or that of their offspring; and to allow for follow-up studies, including prospective studies in which clinical trial patients continue to participate, and future studies that use the trial data as a basis of comparison.

H.R. 52 should acknowledge the stringent requirements already in place for conducting clinical studies and not add new legislative provisions that are unnecessary because they are redundant and may cost valuable time in getting new drugs and better information to patients and health care providers.

#### Concerns about Restrictions on Access to Data for Pharmacoepidemiology

PhRMA is also concerned that H.R. 52 would restrict researchers' access to certain databases that by the definitions in the bill would be considered "protected health information." The entire range of health-related data could come under these restrictions -- from Medicare, Medicaid, and private insurance claims data to state-collected vital and health statistics. These large data bases contain information about many thousands of individuals: about their encounters with the health care system, including their use of hospitals, physicians' services, and prescription drugs, and about the outcomes of their illnesses. This information contains invaluable clues to the causes of illness and about the effects of the medicines already on the market.

We are especially concerned that the bill would restrict access to these data bases even if they do not contain personally identifiable information, but contain codes that could link the information in them to related, but separate, data bases which do contain personally identifiable information. It is impractical to require that researchers obtain consent from patients whose data are contained in such databases. Such a requirement would hinder or prevent research using these databases for several reasons:

1. These studies generally fall below the level of minimal risk criteria that determines the need for informed consent.

2. Informed consent is frequently not feasible because of deceased patients and the difficulty of locating patients in a highly mobile society years after their health information is included in a data base.
3. Getting consent requires identifying and contacting patients which alone may violate the patient's privacy.
4. Using only those patients that can be located and that provide consent will create bias in the results and may invalidate the study.

Similarly, requiring that each use of such databases be approved by a IRB certified by the Secretary of HHS simply adds unnecessary work for IRBs and adds nothing to enhance individuals' protection. If IRB review requirements are added to projects using these linked data, projects in which the patient's identity is at very minimal risk, knowledge about the causes of disease will be delayed, and patients will suffer.

The researcher normally has no interest in the individual patient; encrypted information that would allow all data related to an individual patient to be connected without revealing the identity of that person is generally sufficient for research purposes. The researcher's primary interest in any given patient's data is only the contribution that the data make to the results and conclusions that derive from analysis of the complete study database. Careful encryption of data, and tight security safeguards whenever confidential information is accessed directly, combined with guarantees of confidentiality given by each individual who obtains confidential information, can allow patients' privacy to be preserved without shutting down an entire research activity. Studies in which the use of the key to encrypted data is necessary to link back to other data sources must use special care to ensure confidentiality of identifiable information, and IRB review might be reserved for these studies.

#### The Benefits of Pharmacoepidemiologic Research

Let us look more closely at the kinds of pharmacoepidemiologic research from which we all benefit. Some of this research encompasses what is called "post-marketing surveillance." Such surveillance is necessary, and indeed, often required by the FDA, because clinical trials, limited as they are in size and scope, do not offer sufficient opportunity to observe the rare adverse effects of a drug, much less to quantify their likelihood of occurring and pinpoint the risk factors, especially over a long period of time. But post-marketing research also has other important purposes. It is used to identify unknown benefits of a drug, to compare one drug to another within a therapeutic category, to provide evidence for the optimum dosage or duration or use, and to demonstrate cost-effectiveness to those who must pay for the drug. Concrete examples of such research include:

- Epidemiologic studies that demonstrated a higher risk of hip fractures among elderly taking psychotropic drugs. Several studies using existing databases and records have examined this relationship and heightened awareness about the vulnerability of elderly patients who use such drugs. Injuries are a major public health concern for the elderly, a problem that has significant medical, social, and economic impact.
- Studies that have quantified the risks and benefits of hormone replacement therapy. Researchers used comprehensive data on health care and prescription drug use of nearly 33,000 women over a fifteen-year period. This study showed how small risks of breast cancer become appreciable at longer durations of drug use. Now physicians are able to tell millions of women who face a decision whether to use this therapy exactly what risk they face, based on their age, family history, and other factors. Research along similar lines is possible in the United States, using emerging managed care data bases.
- Research that has showed that restrictions on access to prescription drugs imposed by Medicaid programs not only harm patients, but cost the Medicaid programs money in the long run. In September 1994, Stephen B. Soumerai and his colleagues at the Harvard Medical School reported in the New England Journal of Medicine that restrictions on schizophrenia medications in New Hampshire led to sharp increases in hospitalizations. This research entailed the linking of prescription drug and mental hospital data.
- Large-scale epidemiologic studies that led to the identification of a strong association between Reyes syndrome, a rare but often fatal condition in young children, and the use of aspirin. Demonstration of this risk led CDC and professional pediatric societies to warn against the use of aspirin in children and FDA to require changes in the labeling of aspirin products. The result was a reduction in pediatric aspirin use and a dramatic decline in Reyes syndrome cases in the U.S.
- Another study, of patients with Stevens-Johnson syndrome, a rare but life-threatening illness that is often misdiagnosed, and that has been linked to the use of penicillins, found evidence of increased risk among the users of penicillins. The researchers used the Computerized On-line Medicaid Pharmaceutical Analysis Surveillance System (COMPASS) database, which contains patient-linked Medicaid billing data for the various covered services. The study examined data from three states over a five-year period (1980-1984). Because of the low incidence of this particular disease and the frequency of misdiagnosis, researchers needed to go back to the medical records of selected patients. They used the COMPASS database to identify

patients who might have had the illness, based on their hospital discharge diagnosis; they then inspected the medical records to confirm that these patients actually had the illness, and to see whether they had been given penicillin. Individual patients were never identified in the published reports of the research. Physicians can now be warned to prescribe penicillins with special care, and to be on the alert for the manifestations of this rare syndrome.

- A recent study documenting both the underuse of beta-blockers following myocardial infarction in the elderly, and the serious consequences of that underuse. That study relied on large linked databases in New Jersey and showed that only 21% of eligible patients receive beta-blockers, and that this underuse leads to a 43% excess mortality over 2 years and a 20% increase in cardiovascular hospitalization. This finding is likely to lead to changes in medical practice that will save lives and reduce hospitalizations.
- Research that used medical claims records for elderly patients to recognize that physicians do not always stop antipsychotic therapies before starting treatment with antiparkinsonian drugs. The study data were drawn from Medicaid claims records over a 10-year period. Analysis of these data found that failure to discontinue or modify an antipsychotic regimen occurred frequently and may represent an inappropriate attempt at treating presumed Parkinson's disease.

As these few examples show, this research benefits society substantially and must be allowed to continue. The need for such research will only grow.

#### The Use of Disease and Exposure Registries

Registries that focus on particular diseases are an especially efficient way to collect information to track the effect of a particular drug or treatment, or to compare treatments, over many years or across generations. A number of these registries have been established by federal or state law as a means of gathering useful public health information. The FDA has sponsored several specialized registries to document organ-specific adverse drug reactions. The National Cancer Institute's Surveillance Epidemiology and End Results (SEER) program, a multi-center network of registries, has tracked the incidence and outcomes of all types of cancer in selected geographic areas of the country for some thirty years. In addition, state governments maintain registries of reportable diseases such as tuberculosis. Pregnancy registries have made it possible to pinpoint the relationship of various drugs taken by prospective mothers to serious problems in their offspring and be reassured by the lack of major increased risk of birth defects. Any new legislation or regulations should

ensure that registries continue to be the rich sources of information that they are today.

Conclusion

The research-based pharmaceutical industry respects the privacy of patients and the confidentiality of information about them. We urge you to review and amend the provisions of H.R. 52 so that any changes in federal confidentiality requirements are crafted to ensure that medical research can continue to yield new remedies and better ways of caring for patients.



**Principles for Maintaining Confidentiality  
of Patient-Identifiable Medical Information**

---

Recent developments in the area of information technology have stimulated public concern over the confidentiality of patient-identifiable medical information. PhRMA shares this concern and supports efforts for ensuring the confidentiality of medical information that identifies a specific patient so long as these efforts preserve legitimate access to and uses of such data for research in the continuing discovery and development of medicines. Innovations in medical science, in combination with developments in genomic technologies, are revolutionizing medical research and the future of health care as they begin to reveal the molecular basis of human illnesses. Accordingly, PhRMA proposes the principles below as a guide for a set of requirements to maintain the confidentiality of patient-identifiable medical information, while preserving essential research access to these data. Of course, medical information is used for treatment and payment purposes as well as for research. While these principles address research applications that are critical to the discovery, development and improvement of medicines, PhRMA notes that overly restrictive limitations on access to and use of medical information for treatment and payment purposes could impede the quality of health care available to patients and the effectiveness (including cost effectiveness) of the evolving health care system.

- **Protect Patient-Identifiable Medical Information.** Medical information includes all of the data for an individual patient that describe medical conditions, treatments for those conditions, family medical histories, and any genetic information that is collected through family histories or genetic tests. No distinction is necessary between genetic information and other medical information since the interests of patients are identical for both types of information. Confidentiality requirements should be comprehensive in assuring patients that information identifying them and their medical condition or predisposition to any specific condition is confidential information.
- **Require Informed Consent.** The confidentiality of patient-identifiable medical information should be protected, subject to processes for patient-authorized disclosure and consent as to research uses that may be made of such information. Informed consent requirements for access to and use of patient-identifiable medical information should recognize the value of, and ensure opportunities for, epidemiological, medical outcomes, and pharmaco-economic research that rely on historical, patient-level databases, as well as recognize the importance to breakthrough research of collections of anonymized samples. Reasonable exceptions to the informed consent process should be permitted for example, where the patient's life is at imminent risk, where the patient is incompetent or incapacitated, where there is a question of public health or safety, where such information is used for safety surveillance and reporting, or to comply with existing laws and regulations.

*Pharmaceutical Research and Manufacturers of America*

1100 Fifteenth Street, NW, Washington, DC 20006 • Tel: 202-835-3458 • FAX: 202-835-3595

**Principles for Maintaining Confidentiality of Patient-Identifiable Medical Information**  
Page 2

- **Protect and Promote Research and Development.** Requirements for patient-identifiable medical information confidentiality should acknowledge the extent of existing laws and regulations that govern clinical and other medical research -- including safety and efficacy surveillance and reporting -- and should not impose additional requirements on such research or activities. These laws and regulations already provide assurance that the confidentiality interests of patients participating in such research are well-served through oversight by the U.S. Food and Drug Administration and independent Institutional Review Boards (IRBs). Both voluntary and mandatory safety and efficacy surveillance and reporting contribute to continued safe and effective use of medicines and must be preserved without additional burdensome restrictions. Any new legislation or regulation should also ensure the continued research uses of anonymized databases and collections of samples by clearly excluding such databases from any new requirements or restrictions applicable to patient-identifiable information. Where confidential keys or links to individual patients are necessary in these databases, such keys or links should be maintained separately and securely to prevent inappropriate disclosure.
- **Create Uniform National Requirements.** Federal legislation or regulation embodying these principles should provide a uniform set of national requirements for research that would preempt state laws, but states should retain the ability to specify additional remedies available for violations of the national requirements. This approach will prevent a patchwork of inconsistent and potentially conflicting requirements. Uniformity in the requirements will help to ensure compliance as well as prevent any impediments to incentives for medical research.

2/13/97

Mr. HORN. Well, thank you very much. We appreciate that testimony. We now have Dr. Steven Kenny Hoge, the chair of the Council on Psychiatry and Law of the American Psychiatric Association.

Dr. HOGE. Thank you. Mr. Chairman, I am Dr. Ken Hoge. I am testifying on behalf of the American Psychiatric Association, a medical specialty society representing more than 40,000 psychiatric physicians nationwide. We are pleased to have the opportunity to discuss with you privacy protections for medical records.

Patients come to physicians and entrust them with sensitive, private, personal, and sometimes embarrassing information because they believe that it will be used to help them. Physicians acting in the interests of their patients have controlled access to this information. As the guardian of confidential medical record information, physicians have protected patients' privacy. When third parties inappropriately demand access to medical records, physicians refuse. When the third party's right to access is uncertain, physicians have acted as sentinels, alerting patients that others are trying to seek the records.

Physicians may take steps to protect records even in the face of legal pressures. Physicians have guided patients so that even voluntary disclosures of medical information minimize privacy intrusions. The physician's role as guardian of the medical record has been recognized in professional standards, impressed upon physicians in their training and acknowledged as legitimate by the courts.

Recently, the traditional role of the physician as guardian of patient privacy has come under serious attack. Medical information has increasingly been put to uses that are not intended to serve patient interests. Third party demands for access have increased with attendant risks to patient privacy. Electronic storage of medical information raises serious privacy concerns, since these systems, by design, facilitate access, transmission, and duplication of medical records.

In our written statement, we have submitted several principles that are important to maintaining the privacy of medical records. Let me emphasize the following now. Medical data is generated for the care and treatment of patients and should be used to serve their interests. This can only be done if physicians continue to play an active role as guardians of the medical record.

New information technologies should not be employed to stretch the limits of appropriate access that have been established in professional custom and law. Third, legal and ethical sanctions for violations of patient privacy should keep pace with developments in technology. Existing legal sanctions, such as breach of fiduciary duties, malpractice, breach of implied contract, all help to protect confidentiality and provider patient relationships. These protections, which have been established in professional standards, statutes and case law, should not be undermined.

Appropriate legal sanctions need to be developed to cover insurers, managed-care entities, and medical record data banks that handle and store sensitive medical information but do not have the

tradition of the physician/patient relationship. Throughout your deliberations, please remember that patient privacy is fragile, and that once it is lost, it cannot be regained and its loss cannot be truly compensated. I will be happy to answer your questions.

[The prepared statement of Dr. Hoge follows:]

Mr. Chairman, I am Steven Kenny Hoge, MD testifying on behalf of the American Psychiatric Association (APA), a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I am the immediate past chair of the APA's Council on Psychiatry and the Law.

I am grateful to have the opportunity to appear before you Chairman Horn, as well as Ranking Member Maloney, and the other members of the Subcommittee. At the outset, Mr. Chairman and Representative Maloney I would like to thank you on behalf of the members of the APA and their patients for your past efforts supporting mental illness parity coverage. We very much appreciate your support.

The American Psychiatric Association has consistently argued that federal legislation should not permit the disclosure of confidential information that identifies an individual without the individual's consent with the exception of narrowly-defined emergency circumstances and situations. Congress must insure that broad classes of commercial entities, including information processing companies, cannot release medical records without a patient's informed consent.

We welcome the opportunity to work constructively with you to further these and other principles needed to protect patient privacy and health. We would also like to call to your attention the draft bill now being circulated by Senator Patrick Leahy (D-VT) which we believe offers a reasonable basis for discussing the additional protections needed to protect patients' privacy and health.

#### DOCTOR-PATIENT CONFIDENTIALITY INCLUDING THE CONFIDENTIALITY OF MEDICAL RECORDS IS CRITICAL TO PATIENTS' HEALTH

Confidentiality and trust between a physician and a patient are critical to successful treatment. Indeed, this relationship of trust is one of the key pillars upon which good medical practice is based. As the Hippocratic oath states, "Whatever things I see or hear concerning the life of men, in my attendance on the sick...I will keep silence thereon, counting such things to be as sacred secrets."

In modern times physicians operate under an exacting standard of conduct developed by our profession. These professional rules are supported and strengthened by an extensive and detailed body of case law which provides additional legally enforceable confidentiality standards. It is this trust and confidentiality that allows a full exchange of needed information between doctor and patient on sensitive issues, such as cancer treatment, fertility and sexual function problems, treatment of heart attack victims, as well as the identification and treatment of sexually transmitted diseases.

The procedures for handling patients' medical records have been developed as an integral aspect of doctor-patient confidentiality. Medical records are treated with the highest possible regard for their confidentiality. Thanks to these practices, supported by the courts and legislatures, patients' privacy is protected and the likelihood of successful treatment is enhanced.

Nowhere is the need for confidentiality more clear than in psychiatry. As many psychiatric and other medical experts point out: confidentiality is to mental health treatment what a sterile operating environment is to surgery -- a basic necessity for effective treatment. Often an individual seeks a mental health professional because of the extreme sensitivity of the issue: coping with the death of a loved one, the unraveling of his family life, or feelings of depression and alienation. It would be difficult, if not impossible, for many patients to fully confront these issues unless they trusted the mental health professional and could be confident that the information would be kept private. For these reasons it is critically important to protect the confidentiality of patients' medical records.

In fact, less than a year ago, the U.S. Supreme Court recognized the critical importance of the confidentiality between patients' and their psychiatrists in its *Jaffee v. Redmond* decision. The Court held that: "Effective psychotherapy depends upon an atmosphere of confidence and trust, and therefore the mere possibility of disclosure of confidential communications may impede development of the relationship necessary for successful treatment. The privilege also serves the public interest, since the mental health of the nation's citizenry, no less than its physical health is a public good of transcendent importance." We urge the Congress to recognize and accept the wisdom of the court's decision and be careful not to undermine the psychiatrist-patient relationship through allowing broad and inappropriate disclosure of personal medical information without the informed consent of the patient.

#### CONFIDENTIALITY OF PATIENTS' MEDICAL RECORDS PROTECTED BY THE DOCTOR-PATIENT RELATIONSHIP

Because of the common law protections of the doctor-patient relationship, traditional access to medical records insures a high degree of patient privacy. Access to a patient's medical record is protected by a patient's physician or the physicians on hospital staffs. These records must be viewed in person. In addition, because the medical record is a paper document patient privacy is enhanced because access to the information is limited. Under these circumstances physicians, exercising their strict fiduciary duty to their patients, can protect patients' privacy and refuse inappropriate access. Physicians are also in a position to advise patients on tailoring voluntary disclosures of medical information so third parties can obtain the information they need without intruding on patient privacy. Patients can exercise informed consent to requests for disclosures, and they also have the ability to block virtually any disclosures of their medical records.

#### THE EROSION OF PATIENT PRIVACY DUE TO NEW INFORMATION SYSTEMS CONTROLLED BY ENTITIES WITHOUT A COMMON LAW OR STATUTORY DUTY TO PROTECT PATIENTS' INTERESTS

We are now in the midst of massive changes in the health care field both in how medicine is practiced in an organizational sense and how medical records are developed and provided.

New information technologies have grown explosively, and have been applied to medical practice in ways unforeseen even a few years ago. Perhaps the most troubling development is the computerization of patients' medical records. Likewise, the dramatic growth of managed care has also increased third party access to medical records and the risk to patients of inappropriate and unnecessary disclosure of personal information.

Patients' confidentiality is best protected when physicians in consultation with patients make the critical decisions concerning the release of medical information. And because our laws have not kept up with emerging technologies, new health care entities and even many companies far removed from providing medical care have broad access to medical record information and little legal responsibility to protect patients' confidentiality. There is no shortage of newspaper and magazine stories about an individual's personal and private medical information being seen by others and the breakdown of medical record privacy.

Electronic records pose inherent risks to patients' privacy. Current electronic records are centralized and usually contain all of the patient's medical data. Thus, a single disclosure could have more significant consequences than the disclosure of one doctor's limited records. Likewise, computerized storage of medical information exponentially increases the number of individuals who potentially have access to the information. Even if the record is not transmitted out of the organization storing the records, thousands of professionals, tens of thousands of support staff and other personnel at many different locations have access to computers and thus de facto access to the most sensitive medical records. And in the time it took a person to read a single paper medical file thousands of computer files can be scanned or copied anonymously.

Nor, according to presentations by computer expert after computer expert, can we be confident that any security system will adequately protect the privacy of patient records. It is particularly difficult to protect records from those employed within the organization or system maintaining the data base. Encryption codes can be broken. Users may share their passwords with colleagues or may not follow all the necessary security measures. And not only will audit trails be unable to prevent a disclosure, but the amount of data generated may make it impossible to identify security breaches.

For example, just a few weeks ago the New York Times reported that one law enforcement data system was compromised resulting in the release of informers' names to individuals linked to organized crime. Indeed, even the most technologically secure system can be breached when trusted individuals are careless or seek illicit financial gain.

But the dangers of disclosure are not limited to unauthorized disclosures within the health care system. The computerization of health care records has enhanced the commercial value of medical data. This information can now be easily disseminated outside the medical system for commercial purposes to the detriment of patients.

For example, life and disability insurance coverage companies may acquire this information and deny coverage to patients. And today these companies may deny coverage to a

patient's family members who are "genetically" a higher insurance risk. Even health insurance companies can use the information to deny health insurance access. In some instances medical information will be sold to direct marketers of health products. Not only is such use inappropriate but these companies, far removed from care giving, are likely to utilize fewer safeguards to protect patients' records from additional dissemination. Thus, medical information is no longer being used solely to provide treatment to benefit the patient - it is used against the patient's own interests.

Changing practices by third party payers can also endanger patient privacy. As a condition for health care coverage many patients must now sign unrestricted waivers allowing their medical records to be released. Likewise, many psychiatrists are required by managed care or insurance companies -- either to be a participant in a plan or for the patient to be reimbursed -- to allow the plan or company to review their files, including notes taken during meetings with patients.

If medical records are not adequately protected the impact on patients, particularly psychiatric patients, can be devastating. For example, in 1995 the *New England Journal of Medicine* reported that a Maryland banker, by accessing medical records, determined which of his customers with loans had cancer. He then called in the loans. More recently a Florida public health office employee obtained computer access to 4,000 individuals who had tested HIV positive in confidential medical testing. The worker sent the names of these individuals to several newspapers in Florida.

Because psychiatric records more frequently contain sensitive personal information and because of the continuing stigma that unfortunately still can be associated with psychiatric treatment, the consequences of the improper disclosure of these records is often very severe. In some cases following the disclosure of patient records the individual will stop seeking medical treatment. There have been other cases where co-workers were able to read a colleague's psychiatric report and gossiped and joked about his problems. In one case the employer felt that the person's authority had been so undermined that the employer passed him over for a promotion.

To make the issue more immediate for members of the Congress, public officials and other prominent individuals are particularly vulnerable to improper disclosures of medical information. Several years ago the medical records including information on alcohol abuse problems of a member of Congress from Arkansas were leaked to the press. This disclosure took its toll on voter support in the member's race for Governor, even though the information was subsequently shown to be false. And in 1992 it was revealed that one member of Congress' medical records including information about a suicide attempt were sent to a newspaper and radio station.

These new information technologies do offer possible benefits. But we must provide extensive safeguards so that the traditional trust that has existed between doctor and patient including the confidentiality of medical records is protected. Otherwise, the quality of care that

Americans receive may be harmed. We must not forget that the health and productivity of many Americans depends to an important degree on the confidentiality of the doctor-patient relationship.

#### PROVISIONS NEEDED IN FEDERAL LEGISLATION

The APA strongly supports the fundamental need for protecting medical records. We must have a system focused on protecting patients' privacy and their health. Physicians in consultation with their patients must be able to make key decisions concerning patients' treatment, health, and privacy. For all these reasons federal legislation should not undermine the traditional protections afforded by the doctor-patient relationship.

Federal legislation should protect personally identifiable information by ensuring that the following principles are contained in any legislation passed by the Congress:

- Federal legislation should not undermine the traditional doctor-patient confidential relationship by taking the physician out of the information disclosure process and, therefore, preventing the physician from notifying the patient of attempts to obtain private personal medical information or to inform the patient of potential consequences of disclosure.
- Federal legislation should not permit the disclosure of confidential information that identifies an individual without the individual's consent except in narrowly defined emergency circumstances. Physicians, patients, and other participants in the health care system should not be required to transmit information electronically.
- Federal legislation should not preempt, supersede or modify state confidentiality, privacy, privilege or medical record disclosure statutes or federal or state common law findings that protect patients' medical record information. Federal legislation should provide a "floor" of uniform protection for all personally identifiable medical record information; states should be allowed to continue what is essentially and historically a state's right: to provide stronger privacy protection for their citizens.

The current lack of federal privacy protections for patient medical records needs to be addressed. Certainly H.R. 52, introduced by Representative Gary Condit (D-CA) contains notable protections to protect the privacy of patients. But significant additional changes in this legislation are needed to protect the confidentiality of the doctor-patient relationship and more specifically the confidentiality of patients' medical records.

The APA is very encouraged by the draft proposals being circulated by Senator Patrick Leahy's office. This legislation contains several key provisions not found in legislation now before the Congress. Patients are given basic rights to protect their medical information; most notably they have the right to segregate information in their records and with narrowly defined

exceptions to control whether such information can be released, and are provided explicit notice of these rights. They also can choose to have their records kept outside of computer databases where the risks of possible disclosure are greater. Equally important, under the Leahy draft bill the federal law would provide a minimum acceptable floor to protect patient confidentiality, and thus any individual tougher or more restrictive state laws to protect that state's citizens would not be preempted. We urge the subcommittee to review the key privacy protections in the Leahy draft.

In closing let me reiterate the particular importance of protecting the confidentiality of the psychiatrist/patient communication. Any interference with this relationship impairs the ability of a psychiatrist to help his or her patient. The APA urges the Subcommittee to accept what court after court has recognized as a legitimate zone of privacy - the psychiatrist/patient relationship - and protect the confidentiality of an individual's psychiatric medical records.

Thank you again for this opportunity to testify, and we hope to have the opportunity to discuss these issues further with you and your staff.



Health Insurance Association of America

**Committee on Government Reform and Oversight  
Subcommittee on Government Management, Information and Technology**

**Legislative Hearing on  
"Medical Records Privacy : H.R. 52"  
June 5, 1997**

**Written Statement by the  
Health Insurance Association of America**

The Health Insurance Association of America (HIAA) is a trade association representing 250 commercial health insurance companies, managed care plans and Blue Cross Plans. Our member companies provide products such as health insurance, dental insurance, disability income insurance, long term care insurance and Medicare Supplemental insurance.

We are grateful for the opportunity to provide a written statement about health confidentiality issues to the Committee on Government Reform and Oversight's Subcommittee on Government Management, Information and Technology.

**General Comments:**

HIAA whole-heartedly agrees that protection of personal health information is vitally important to the people of the United States and is an important aspect of health care reform. Although the Act's provisions are well-intended, HIAA is concerned that its operational implementation could impose a heavy administrative burden on health plans and providers. Such an administrative burden could result in increased costs to consumers and confusion to patients. It is important that health insurers be able to use health information for the legitimate purposes of evaluating and paying claims, case management, utilization review and peer review and for the underwriting of disability, life and certain health policies.

Our member companies have much respect for the confidentiality of health information which is under their control for payment purposes. Typical policies and procedures involve the signing of confidentiality statements by health insurance company employees which expressly forbid them to disclose confidential data about patients. Most importantly, such statements set forth consequences, so that if improper disclosure occurs the employees are

terminated from employment. We respectfully request that, as the Committee reviews privacy legislation, the following points be carefully considered:

1. The legislation be consistent with the ultimate goals of Administrative Simplification in health care which are:
  - to increase efficiency
  - to decrease costs
  - and, most importantly, to improve patient care.
2. Please be mindful that well-intentioned, but onerous, administrative burdens placed on providers or payers can increase costs to patients.
3. It is important that private recommendations be flexible enough to suit the fluid organizational changes of the health care marketplace.
4. The recommendations should exercise caution with respect to the procedures for correcting or amending protected health information. There have been legislative proposals which imply that patients are qualified to make changes to medical records. We believe that any changes to medical records should be managed through a patient's physician, or other provider, who is appropriately qualified to make determinations regarding such changes.
5. It is very important to our member companies that Federal Law supersedes state law in the area of privacy of health information. Our members have multi-state operations and it is a difficult and expensive administrative burden to comply with varying state laws.
6. Lastly, we firmly believe that privacy protections should allow for comprehensive and coordinated patient care services in network-based health care plans. Such health care plans offer coordinated health services to patients and therefore it makes sense to enable patients to provide a single authorization for:
  - health care treatment,
  - payment for services by plans,
  - plan utilization review,
  - and, plan health management services.

This single authorization enables coordinated patient care and facilitates efficient and appropriate sharing of information among health care providers and plans in order to provide patients with high quality health care services. This is particularly important in the case of integrated medical records.

**Comments about H.R. 52:**Subtitle A –Duties of Health Information TrusteesSection 101 Inspection of Protected Health Information

This section appears to allow an individual broad access to all of the health information the insurer has, but in contrast to other laws in this area, there is no clear exception for information collected in connection with claims investigations or to prevent fraud. The serious problem of health care fraud and abuse necessitates a specific exception for claims investigations and other anti-fraud activities.

Section 102 Amendment of Protected Health Information

This section implies that patients are qualified to make changes to medical records. Any changes or amendments to medical records should be managed through a patient's physician who is appropriately qualified to make determinations regarding such changes.

Section 104 Disclosure History

Patients routinely receive medical services from a variety of providers such as primary care practitioners, medical specialists and allied health personnel. In today's fluid health care organizational context, and especially in managed care settings, patients may be treated by a variety of medical service providers. This section implies that in the course of providing routine medical services, providers must maintain detailed disclosure records. This is an unreasonable requirement. Part B of this section needs to include an exemption for medical treatment provided to patients.

Subtitle B - Use and Disclosure of Protected Health Information

The Act requires that health plans and providers obtain written, specific authorization from patients prior to disclosure of patient's health information. The information to be disclosed and the recipient of the information must be specifically named or described in the written authorization. This provision means that patients need to give an authorization for each physician, medical specialist, allied health person or health plan person who might have the need to review patient health information. For example, in a network-based managed care arrangement, it is conceivable that a patient would need to sign an authorization form for each of the many persons who would ultimately see the patient's medical record. Such requirements can delay the delivery of health

care services to patients which can potentially adversely affect the quality of medical care provided.

Subtitle E – Enforcement

We find it troublesome that the Act creates a private right of action and the right to obtain punitive damages. Such provisions raise the potential for a large increase in frivolous litigation. Regulating health information does not require creating a new cause of action. We suggest that broad exceptions should exist for inadvertent disclosures and those made in good faith, and plaintiffs should be required to show specific harm.

Mr. HORN. We thank you very much for that statement and I am going to put in the record the comments of the Health Insurance Association of America. They were invited to testify, but they were not able to make it, so their statement, without objection, will go in the record at this particular point. They raise some interesting questions, which we might get into during the question period here.

Let me just ask all of you here, what type of penalties are appropriate for individual medical privacy rights and if someone violates them, what do you suggest? Let's just go right down the line.

Ms. Goldman.

Ms. GOLDMAN. Thank you. Well, I certainly believe—

Mr. HORN. You did the right thing. You pulled the microphone toward you. All those microphones need to be pulled toward you. This was built in the 1960's, but they use the 1890's sound system, so we have a problem.

Ms. GOLDMAN. I certainly believe that any Federal law should incorporate a variety of remedies. One remedy is not going to be sufficient. There should be a private right of action that gives an individual the ability to come in and bring a lawsuit against someone who has harmed them. Also, I think that an appropriate Federal agency, such as HHS, should be able to assess a civil penalty, so if the individual can't afford a lawyer, the Government can come in and say you have done wrong. And I also think, under very egregious circumstances, there should be criminal penalties as well.

Mr. HORN. Well, if there is a criminal penalty, what should it be? I mean, is it a misdemeanor or is it a felony, let us start there.

Ms. GOLDMAN. Well, I think that by the time you reach the level at which you would be liable for criminal penalty, I think you should be looking at a felony. A criminal penalty, particularly under a number of the proposals that are out there, would be where there has been intentional, malicious disclosure of personal information, where there is a course of conduct over a period of time, the person—

Mr. HORN. Pattern and practice.

Ms. GOLDMAN. Pattern and practice, flagrant violator, should certainly be a felony.

Mr. HORN. What is your feeling, Dr. Palmisano?

Dr. PALMISANO. Thank you, Mr. Chairman. The American Medical Association believes penalties and sanctions for unintentional disclosures of identifiable patient information, where the disclosure does not result in demonstrable harm to the subject of the disclosure should be commensurate with the violation. Repeated such unintentional disclosure should receive stronger penalties if they indicate a negligent business practice.

Penalties and sanctions related to improper disclosure for commercial purposes, profit malicious purposes or where there is significant patient harm should be more stringent. In addition to monetary sanctions, legislation could include the loss by a data base company, for example, of its privilege to hold or transmit protected medical information, thus reducing the potential for companies to accept the monetary penalties for improper, intentional disclosures, as a cost of doing business.

In other words, we don't want them to say, well, gee, there is this little penalty. We will just pay it because we are making so much

money here, but they would lose the right to function in that capacity in the future.

Mr. HORN. Has your association considered the thought of compulsory arbitration, rather than going through the court system? Some associations do this. I mean, the patient would sign either mediation, which is not compulsory or a compulsory arbitration agreement. Rather than going into court on some of these, they would sign that if something happens to the record, let's say, you would have compulsory arbitration, and that would be, perhaps, an arbitrator picked by the patient, one picked by whoever, the doctor or hospital, whatever the violation source is, and the two usually pick a third.

Dr. PALMISANO. The American Medical Association for years has been in favor of alternative resolution mechanisms to the current court system. We believe it is expensive and very inefficient and that does not serve both sides very well, in our opinion. In this situation, I guess there would be two issues. The first issue would be how would you resolve the issue and we certainly have been in favor, as an association, of voluntary binding arbitration?

For instance, in Louisiana, we have that as an alternative to the court system, if both sides agree prior to the event occurring, and there is a period of time, a cooling off period where you can change your mind, but after that, it is a binding arbitration. So in general, we are in favor of that. The next issue goes to the penalty phase of it. Would the arbitrator have available to him or her certain penalties that would be mandated to follow, based on how egregious the act was and so on?

Mr. HORN. That would be the civil side of it, certainly. Obviously, they wouldn't be getting into the criminal side. But you also have the sort of rent-a-judge approach in many jurisdictions where X judges regularly decide very difficult disputes and both parties agree and it gets it out of waiting 1 or 2 or 3 years to come up in some court systems.

Dr. PALMISANO. In general, the AMA has been in favor of such methods, where we could have alternative ways to resolve that. We just want to make sure there is fairness, due process and so on.

Mr. HORN. Dr. Johns, any feelings on this?

Ms. JOHNS. Mr. Chairman, part of our model legislative language and key provisions for national regulations in regard to this included civil and criminal penalties. Now, as far as distinguishing felony and when that should occur and so forth, I don't believe that we had gotten into that particular detail. I do feel comfortable in testifying, however, that the provisions, as they are stated in H.R. 52, is something that our association supports.

Mr. HORN. Dr. Gabriel, do you have any thoughts on that?

Dr. GABRIEL. Not really. I would agree with what has been said before. I think it really depends a lot on the type of abuse, the motivation for it, whether the abuse is for commercial reasons, whether there has been patient harm, and I can tell you that in our own institution and I know in many others, even the mildest level of abuse results in termination of employment. So I think there has to be that and that the IRB has an important role in monitoring it and making sure those abuses do not occur.

Mr. HORN. Dr. Andrews.

Dr. ANDREWS. Well, first tight controls over data within the research setting are effective in preventing these types of violations. However, we do also concur that there should be penalties and that those penalties should be commensurate with the disclosures. PhRMA has developed no specific recommendations about penalties.

Mr. HORN. Dr. Hoge.

Dr. HOGE. I think the only thing I would add, I think it is important for all of us to keep in mind confidentiality is sort of a tricky thing to regulate, that once privacy has been breached, suing someone doesn't do you much good. The fact they are punished may not do you much good. Internally, in a hospital, terminating an employee, I think obviously makes a lot of sense, but what we see over and over again is that the result of bringing a lawsuit or seeking some kind of legal redress would be wider dissemination of the information that the person wanted to keep confidential in the first place. So there is a little difficulty here.

At the APA, we have seen criminal penalties wax and wane in various versions of the bills. No penalty is too severe if the transgression is severe, assuming the underlying rules are set appropriately.

I do want to add one other comment. You asked the earlier panelists if they had any disagreements. I think the biggest fault line I perceive in this issue over the last 3½ years pertains to the pre-emption issue. I think it is—my view is it is beyond a doubt, the APA has spent countless, hundreds of thousands, if not millions of dollars over the last generation, developing case law, statutes in States all over the country.

We were instrumental in the *Jaffey v. Rudman* case. It is cited prominently in your draft bill. I think it is not correct to say that privacy is not protected in this country or that the States aren't doing an adequate job. Many States and many courts are doing a very adequate job. So I think the pre-emption issue is an issue, and I think to put the whole moose on the table, that the people who are interested in pre-emption are interested in the efficiencies that pre-emption would provide, not in privacy protection.

I think it is clear if a State wants to come along and raise the bar from any Federal law that might be passed, that that can only help patient privacy. I don't see any logical way of getting around that conclusion. So I think we need to understand now we are talking about privacy versus efficiency, and obviously the APA is going to come down on the side of patient privacy.

Mr. HORN. I note in the Health Insurance Association of America testimony, this is the last time I will cite it, but it is relevant to this question. They say under Subtitle E, enforcement of the Condit bill: "We find it troublesome that the act creates a private right of action and the right to obtain punitive damages. Such provisions raise the potential for a large increase in frivolous litigation. Regulating health information does not require creating a new cause of action. We suggest that broad exceptions should exist for inadvertent disclosures and those made in good faith and plaintiffs should be required to show specific harm."

Are there any reactions, anybody, to that? It is a little different than some of your testimony, so I thought I would throw that in for the record.

Dr. PALMISANO. Mr. Chairman, just one comment about frivolous actions. The American Medical Association is on record repeatedly that we are in favor of anything that discourages frivolous actions and certainly in the Health Care Quality Improvement Act, which created certain protections for peer review and also created the National Practitioner Data Bank.

There is a provision in there that if someone files a claim without merit, and so on, that the individual can be sanctioned. And certainly I think in any legislation that we need to look at situations for people who don't really have a basis for it, and do this just to harass. So we would be in favor of something of that nature.

Mr. HORN. That is a serious problem, without question, in some types of litigation. I think I said a year ago, when we were able to override the President's veto, when he was sort of defending that, 1 or 2 years ago, I guess it was, the fact is the American Bar Association, if it wants to be a professional organization, ought to be dealing with these matters. That is what professions are supposed to do, regulate their members. We haven't seen it yet. Maybe some day they will decide they are a profession and do something about it. It is despicable, some of the filings, absolute blackmail. And that is what has Congress upset in this area.

For those where you have a true pattern and practice, that is something else. However, where you simply have somebody fishing around, trying to, in essence—and I went through this as a university executive and president. They filed suits and they figure you will buy them off at \$10,000 a month or something, and if you got 50 suits filed, that is a pretty good income. So that is serious, how we deal with this and try to get the people that are really violating the law, versus the sort of snooping expeditions or whatever we call it, where we just have that kind of conduct by a small handful, less than 1 percent or one-tenth of 1 percent, but enough to be annoying. So let us see here.

All the panel has really taken a look at this one. Under H.R. 52, Secretary of Health and Human Services would be required to develop standards for maintaining the confidentiality of patient health records. Health care is provided in a wide diversity of settings in the country and they are pretty well represented here. We could have had another panel there 50 feet long and health care is provided in these settings, ranging from single practitioners in rural areas who provide care at multiple locations to large centralized hospitals. Can we expect a single records maintenance standard to be appropriate in all these different settings? If not, how should we take the differences into account?

Any feelings on that? Let's start with Dr. Hoge.

Dr. HOGE. Are you asking me about my feelings because I am a psychiatrist?

Mr. HORN. Sure, that is what I hear psychiatrists ask about. My one course in psychology taught me that.

Dr. HOGE. I have some thoughts on that. I think it is extremely difficult to regulate the use of medical information in all the various contexts.

You mentioned going from research to data base to provision of health care, and I think that is one way in which many of the draft bills have gone off course. We know a lot about how to regulate physicians because we have had physicians and patients for as long as we can remember, and we have had case law and profession—we have had professional standards and professional training now for, again, as long as we can remember, as long as our grandfathers can remember. So we know a lot about that.

And the bills kind of take an outline from how we think about doctors and try to make everyone else fit into that outline. I don't think it does a very good job. I think this is a strange way to make a law. I think it would make a lot more sense, if we need a Federal bill concerning physicians and it doesn't undermine existing State laws and case laws of malpractice, so be it.

I think what is really needed in 1997 and in the future are laws that regulate data banks, managed care companies, insurers, and all of the entities now that have come to hold medical information that 30 or 40 or 50 years ago no one had even heard of these entities. I think it is particularly important because of the march on information technology. If you think up an information technology journal, you will see that some people believe that the insurance record and the medical record will be the same thing when we have all the computers up and running and software available. I find that a frightening Orwellian future. So I think what we need is some sort of regulation that starts to look at these other entities.

I think we also need to keep in mind, like the various panelists earlier acknowledged, the physician should be the only one to change the record. They know the patients. They know what they are worried about, their privacy concerns, and their health care problems.

Our professional standard requires that physicians look out after the best interest of patients. That is not true of any of the other entities that I have mentioned. So we need to have—just like the physician should have certain prerogatives in that setting, with regard to that question—certain prerogatives with regard to the use, disclosure and dissemination of all health care records. Data banks should be relatively restricted and tightly regulated ways in which they can use health care information.

Mr. HORN. You mentioned Orwell. Do you see physicians sort of using their own personal code in some of their records so if they did get misused by one of their staff or any of the food chain along the way, so to speak, that it would be very difficult to know what that number or that letter meant unless you had a subpoena and you were a witness in court where you were asked to translate it, something like that? But the average person who wants to make trouble in the publicity sense would not know what that means.

Dr. HOGE. Well, of course we spend 4 years in medical school learning terms that no one else can understand.

Mr. HORN. That is the making of a profession.

Dr. HOGE. Right, make up your own language.

But the serious answer to that I think would be this: I hear psychiatrists increasingly tell me I have changed the way I write my notes now, changed the way I keep records, because I don't know who is going to see it. When the insurance people come in and re-

view the charts, I don't know if the insurance reviewer is really a friend, a neighbor of the patient. Some of that gets entered into various data banks. I don't know who is going to see that. So we have a number of things.

We have patients who say, I have insurance and it does cover some mental health care, but I don't want to use it because I know it is going to go and the records are going to be reviewed by—it may make its way back to my corporation because we have our own in-house review of insurance payments. So I don't want to use it. I want to pay out-of-pocket.

Of course, it is a sorry state of affairs in this country that we don't have mental health coverage on par with many other countries, however even when we do, people feel they can't use it. Prominent politicians, on occasion they have many ways they can be hurt by mental health treatment records.

Then I have physicians telling me, psychiatrists telling me I don't put very much in the record now. So if I want to go back now and look 5 years ago, my records are very detailed. But 5 years from now, if I want to look at my record, I am not going to have exactly the same kind of information. It's going to take more reconstruction to get to that.

So what we are seeing, because of this march of technology, the lack of regulation of insurance companies and other people, I think we are seeing an erosion of the quality of medical recordkeeping in this country already.

Mr. HORN. Let me throw another question into it, and maybe you can all just go down the line and answer two of them, because it is relevant here.

That question is, should a Federal medical privacy law such as we are considering, not necessarily the one we are considering but a law, pre-empt all State laws, or should we—and a lot of Californians feel this way when it gets to air pollution and control of frozen chicken and other hearings we have held around here—if the State has a stricter standard, to let the State standard apply if it is stricter than the Federal standard?

And I would also like to hear from all of you some time today, is there a State law that you think is the best law in this area right now? And of course States, as you know, have a system, if we have got a good law, trying to get the uniform code activity of other States with that model statute across the country.

So we face the problem of what is that relationship if we do something in Federal law and we have sort of given the HHS Secretary an anointment which maybe she shouldn't have, and maybe Congress ought to battle these things out. Because they don't have to listen to people. We do have to listen to people.

That is where we are on that one, and I would just like to know what your feelings are in that whole jumble: What is the best State law and should there be Federal pre-emption, et cetera?

Dr. HOGE. On what is the best State law, I think that is difficult to sort out, because much of the law is incorporated in either State laws or it is instilled in professional case law and practice, and that may vary somewhat from jurisdiction to jurisdiction. But, increasingly, physicians are held to a single national standard. So I think

finding out where the best practices are and the best regulation will be a very, very difficult thing to sort out.

Regarding pre-emption, as I alluded to earlier, I think that is the major fault line in this legislation. Because many of the bills that I have seen I think would erode existing privacy protections in this country, with regard to physician/patient relationships and the systems that physician control, which are held to, I think, a fairly stringent standard under malpractice law and existing case law.

I think we need to keep in mind that the only arguments for pre-emption are arguments of efficiency and ease of transmission of information. There is no way to justify, if you do come out with a law which sets the bar at a certain level, if a State wants to raise the bar, that can only be protective of privacy. I don't see any privacy argument against a nonpre-emptive Federal law.

Mr. HORN. Dr. Andrews.

Dr. ANDREWS. Yes. First, I would like to respond to your earlier question about different controls in different settings.

There are certain universal principles about data protection such as the need of safeguards for personally identifiable data and penalties for severe breaches as we discussed. But the specifics are very different, as you mentioned earlier today, and in writing the legislation, the devil really will be in the detail; and we should be extremely careful in those details should they be put in the legislation so that those details do not inadvertently create barriers to research that will ultimately benefit the public in the long run.

Regarding specific State legislation, first of all, let's not use Minnesota as an example of model legislation. I think that was probably very carefully crafted legislation and yet, as you have already heard, the Mayo Clinic has an incredible record of some of the most distinguished, productive, and tightly controlled research; and we have already seen that the Minnesota law creates some impediments to future research using that valuable resource.

Regarding pre-emption, one of the compelling reasons for Federal requirements is to provide a uniform set of rules; and if individual States are permitted to add additional requirements, then the benefits of those uniform rules may be lost and researchers will again be faced with an inconsistent patchwork of requirements that may impede research and hurt patients. We need to remember that much research today does not know geographic boundaries and involves multiple States and multiple countries.

Mr. HORN. Dr. Gabriel, how about it, in terms of the single records maintenance standard appropriate in all settings? And do you agree that the Minnesota law has those major problems you have heard about from yourself and others?

Dr. GABRIEL. I absolutely agree. In response to both of your questions, one size does not fit all. Integrated health care delivery systems like Mayo are different. A patient can access the system at 100 different points, can see numerous providers. There are dozens of, referrals going on all the time. It is hard to even define what constitutes a point of access. So I don't think the same rules can apply to an individual provider as to integrated health care delivery systems like Mayo.

There really has to be a way to facilitate the appropriate flow of information, because that is our strength, is that we can do all of

this, that the lines are going in all different directions to the benefit of the patient.

In fact, with our recent experience with the Minnesota law, we have a partner in Rochester, a much smaller center, who have had far fewer problems. Because everyone comes in the same front door, and their system is basically sticking a red sticky on the chart, and if you see a red sticky, don't read the record. But we have to have a very complicated information management system that is constantly updated, and we are always looking at where the patients are going, so it is an entirely different kettle of fish.

We favor pre-emption to the State law, again, for the same reason. Mayo operates in five different States. Our patients go back and forth from one State to another. Our research covers more than one State. So it just makes a whole lot of sense to have uniformity.

Mr. HORN. If Minnesota law doesn't meet the test of your particular standards, are you aware of any State law that comes closer than Minnesota?

Dr. GABRIEL. I am not.

Mr. HORN. OK. Well, I would say to all of you when you go back on the plane or train or bus or whatever and have some thoughts in this area, please write us. We will put it in the record at this point and others. Because what we are interested in is the best thinking in this area that is going on. Obviously, six people don't represent all of the best thinking in America, but it is a start.

For your professional associations and their high-paid staff, we would certainly welcome actual line-by-line criticism of the bill. That might not be the bill, but that is a start—or the Slaughter bill or whatever you want. And we would like your specific criticisms so we can get the total picture.

We don't enter into this with a lot of preset ideas, except maybe on frivolous lawsuits. But we would like your thinking line-by-line. If you have a thought, don't be bashful.

So lets ask Dr. Johns. How do you feel on the diversity of the setting? Do you think we can do a law that has the basic standard that can cover all that diversity? And if you know of a State law that does this well, we would like to hear about it. And do you think there ought to be Federal pre-emption?

Ms. JOHNS. First of all, HIMA is in favor of pre-emption. And I think when we look at the issue of confidentiality we also have to separate issues of confidentiality and security practice.

In regards to the confidentiality in H.R. 52, we are looking at inclusions of key provisions in regards to health information, as opposed to carving out regulations for specific types of entities.

New entities in the health care industry arrive on almost a daily basis, so to regulate individual entities does not, in our minds, seem to be either feasible or reasonable. However, focusing directly on the health information that can be within any type of entity is the important part of H.R. 52; and we have key provisions such as access, such as disclosure, such as limiting information in order to—for specific use to perform a specific responsibility, and also provisions on redisclosure. So from that aspect, looking at it from that perspective as opposed to separate entities we think is very, very important.

We also feel, as I mentioned, that we need a national standard. We don't have that now. And we need to—it is so imperative that we begin to address this issue on a national standard.

Also, data does cross State lines. Integrated delivery systems themselves may have facilities in two, three, four, five, and many more States. So the issues regarding the health information need to be standardized across the country.

Another point that was made by Dr. Hoge is the issue of patients feeling comfortable with being able to confide in their health care providers. And certainly previously I pointed that out in our testimony, that one of the mainstays of confidentiality is this confidence that the patient has in being able to share information.

The kinds of situations that we are encountering today where patients withhold information and providers are not as specific with regards to their documentation result from not having general preemptive legislation that ensures all of us that we will have confidentiality and privacy.

In regards to identifying a specific bill throughout the country and the State, I am not aware of that; and I am not prepared to provide that information at this time.

Mr. HORN. Well, we would certainly welcome any thoughts your organization has. You have got a vast group out there. Or complaints where—please don't take this portion of law; it doesn't work.

Ms. JOHNS. We would be happy to provide that.

Mr. HORN. Dr. Palmisano.

Dr. PALMISANO. Thank you, Mr. Chairman.

Regarding pre-emption, the American Medical Association is of the opinion that without a showing that the proposed Federal standard would be properly protective of patient privacy, any Federal law should provide a floor rather than a ceiling when applied to patient confidentiality protections. It is understood that there are many who believe that there should be a uniform Federal standard to facilitate electronic data interchange.

The AMA is concerned, however, that heightened standards will be lost to Federal legislation. If, however, the law is high enough to secure protection of patient information in the Federal language, the AMA would revisit the pre-emption issue.

I think Dr. Hoge's comments are issues we share concerns about. We think there are many concerns in States, and tomorrow they may pass a new law in a State that is ideal, and it is perhaps quicker to go through a State if we see a problem with confidentiality and raise a standard at a State level. So we think at the present time it should be a floor, not a ceiling.

Regarding the uniform coding issue, we don't have a problem—for simplification, we don't have a problem with the provider identification number. For instance, the American Medical Association has an identification number for physicians. We would like that to be considered as a number that would be appropriate for physicians.

Regarding a patient identification number for simplification, we are very much concerned about that; and we continue to study that. Our testimony in the past and continues to be at the present time, we are opposed to a unique patient identifier because it can

too easily be linked up with Social Security numbers and other mechanisms that would allow someone who doesn't have the right to get there to gather a lot of information about the patient. We have a lot of concern about that.

The other issue on uniform coding and so on, we certainly think that the current procedural terminology that is in place, CPT coding system, it is in common use; and we hope that the choice of coding system will allow for the CPT to compete fairly with any other system that is being considered.

Regarding the wide range of practices throughout the United States, from clinics to small practitioner, I certainly don't want us to forget the small practitioner who may be a family practitioner in a small town, and this individual finds the administrative burdens continue to increase. Managed care has drastically affected the practice of medicine throughout the United States, and any other burdens might cause that practitioner to say it is not any fun, I can't do for my patients what I need to do for my patients, and we will see physicians retiring earlier, leaving communities, and that is a problem.

So any law that would eventually be passed by Congress, we would hope that it would not create burdens on individuals who elect not to get involved in that methodology. If they are working just in their area and not transmitting the data, it would be on a voluntary basis. So someone doesn't say, now I have to buy a very expensive computer system; I have to bring in consultants. And many times, after that is over with, the physicians find out after they have spent a lot of money and they are not any better off. In fact, they are worse off because nobody understands the system.

So we want to make sure that those who elect not to be involved in transmission of data to central data bases, they don't have to do that. And whatever comes out of Congress we are concerned about some clearinghouse in the sky where all of this data is going to be there. We are concerned about someone getting in and cracking into that information; and, as you have heard multiple times today, privacy has to take the No. 1 position over efficiency.

Mr. HORN. Since I grew up in rural America, I am very sympathetic with the type of examples you have cited and others.

Now it seems to me the AMA, as a professional association, may sponsor workshops in which physicians or their office administrators could be educated and trained and specialized software. Do you develop software that can be used nationwide that would solve a lot of these problems? We do not want to drive that poor individual physician who was taught to do good in medical school out of serving rural America.

Dr. PALMISANO. Yes, sir, we have extensive programs at the State level and the American Medical Association level.

And I know I will hear this—I am in practice before the colleagues, and when I get back and sort of give them a recap on how we are participating, our great civics lesson, in America, the greatest land in the world, how through democracy we can give our voice. And then my partner, who is my mentor in training, he just always looks at me and says, come back to the real world here. Do you realize what we have to do here? Do you realize the adminis-

trative burden? Why I don't leave here until 8 at night even though I have an office manager. We have to hire consultants to come in.

He is as sophisticated as anyone I ever met with computers, with the methodology to make sure everything is kept proper. But he says it is a tremendous burden.

So I always listen sympathetically and say, "well, I know, but we just want to make it simple and make sure our voice is heard."

And he says, "we already know how to do it. The problem is the rules keep changing."

For instance, when the fraud alert two came out, I had occasion to be treating a very prominent member of our community. His wife and he had some connection with the judicial system, and he was upset because I was an hour late. I sent word because there was an emergency I had to run into the operating room and lend a hand with a very critical patient, and when I got there he started to lecture me as he often does.

And I like him a lot, and I listened, and I said, "Sir, if you would sit down and help me understand an alert I just got from our Federal Government about fraud alert two, which had to do with if you write off the balance of a patient, that is considered a crime." I said I don't quite understand that. It looks like it says that in English. And he said that just can't be so.

So I went and treated his wife and came back, and he says, "I just can't believe that." I said, "That is part of the administrative burden." We have patients that come up. I don't want to do means testing on my patients when they say, "Doctor, can you just accept the assignment?" Sure, I will accept the assignment, but now I have to do means testing.

Those are the many, many little things that keep coming up; and one little thing doesn't sound like a lot, but if you add another thing and another thing and another thing, that gets to be a lot.

I am trying to treat the sick and help people. When I can't cure them, I want to comfort them. But I am just getting overwhelmed by the burden. And no matter what comes out, whatever we call it—we can call it simplification, call it privacy, but we don't want to create a burden that is more burdensome. We don't want to create a system that allows someone—like in other countries that kick down the door in the middle of the night and say I am just here to inspect and make sure there is no fraud going on in this home. This is the land of America. So that is our plea.

Thank you.

Mr. HORN. Well, I know a lot of doctors in my urban community that completely agree with you about the burdens that have been placed on the private physician; and, as you suggest, some of them are being driven out of the profession by simply the water treatment harassment that they are getting. Whereas one or two drops wouldn't bother you, but when it adds up to Niagara Falls coming in your direction, you worry a little bit.

Ms. Goldman.

Ms. GOLDMAN. The position that I am taking on pre-emption in this Congress is slightly different than the one I took last Congress, and I would like to just lay out how I have arrived here.

I have come to believe that pre-emption of State law in the privacy area is not the right approach to take. First of all, the States

that currently have laws on the books that deal with access to records and allow people to limit disclosure of their own records are being complied with right now by the people sitting at this table who say it would be unworkable to have a Federal law that allowed for States to pass those. Right now, we have 50 different States with 50 different approaches, and people are not only managing to comply with those different laws, they are flourishing and doing quite well.

The second thing is that, with the passage of a Federal privacy law, regardless of where the floor was, most States, I think, would feel that the issue had been addressed. The States that have been extremely active right now in passing legislation are doing so because there is a vacuum, because there is a serious need, either because there has been a story in their State or a problem in their State and they have to address it.

And the States that have been particularly active are your home State, Mr. Chairman—California—Minnesota, New York, and Massachusetts. Where they have active consumer groups, the States' attorneys general have been active in those States; and while they may have passed laws that are imperfect from the perspective of the pharmaceutical industry and the health information industry, they are fulfilling a need.

So I would say in this area we cannot only create a floor which is a high floor so those States that are weaker or problematic are, in effect, pre-empted, because the State law must meet that floor, but it would discourage other States that would say "finally Congress has addressed the issue, we don't need to be tinkering with it." And I think it would allay a lot of concerns that the pro-pre-emption folks have been pressing, which is how would we comply with a few variations in the Federal law, when right now they are dealing with 50 variations.

The only other point I want to make is to pick up on something Dr. Gabriel said, that one size doesn't fit all. One size probably doesn't fit all, that if we do create a Federal floor—excuse my New York accent—

Mr. HORN. It is either a Freudian or Jungian slip.

Ms. GOLDMAN. No, it is my accent. If we do create a floor which is a high one, I think then only States where there have been very serious, egregious violations and States with particular instances they want to address will enact legislation. The context is very important as well.

I have worked in the privacy and civil rights area for a decade, and there is no other Federal privacy law or Federal civil rights law that pre-empts State law, and I think it would be a dangerous precedent to set. Those laws recognize that the privacy law is meant to do something good, to protect an interest that is considered vital to a national interest; and if a State finds it is important to go above that floor, they should be free to do so. I think particularly in this instance it would be wrong to constrain the States.

Mr. HORN. OK. Any other comments you have heard your colleagues on that you would like to correct now that we are down to number 6?

Dr. HOGE. No corrections.

I might bring to your attention Senator Leahy's draft bill which is, I think, going to be introduced in the next couple of weeks which I think provides a reasonable platform on many of these issues.

Mr. HORN. We are in contact with the Senator's staff on that, and we have worked with Senator Leahy on various occasions.

Let me get back to fraud detection. One criticism leveled at H.R. 52 by the insurance community is that it would inhibit antifraud activities. Insurance companies would be limited in the claims investigations they would perform. Should there be a specific exemption for claims investigation and antifraud investigations? Anybody have a strong view on that?

Dr. HOGE. Yes, I do. It is not clear to me why the insurance industry would say that. There are many countries that have national health care systems that don't intrude on patients' privacy the way they are proposing. There are many ways of detecting fraud and abuse through billing patterns, number of billings today, without getting access to identifiable, protected, sensitive health care information.

It is just being done throughout the world in other ways, including Canada which has a society not so different from ours, again by looking at patterns of billing rather than specific, identifiable information.

So I think once they have justification—

Mr. HORN. Let me stop you right there. Let me be sure I understand you.

Often what we are talking about is some software has been developed that when a certain type of operation is performed, lets say, there are certain things that relate to that; and one can look through the bill in a systematic way and even by software that would say, well, gee, I wonder why this was done. That isn't normal or usual with this particular operation.

To give you a real horrible example, a woman, not in my district, but in a neighboring district, wrote about going to a hospital, having a particular type of operation she went in for. In the process of being there, they also did a mastectomy, claimed the bill. She thought that was strange since she had had a mastectomy 10 years before.

So, obviously, there are some things thrown on these bills by unscrupulous hospitals and unscrupulous physicians and unscrupulous HMOs, whatever. There are a few bad apples we always find somewhere, and that is sort of what we are confronted with. I don't see how you deal with that operation without knowing the name of the patient.

Dr. HOGE. Well, I think the example you gave probably would be sufficient to get a court order to get access to the records or maybe it is the first step to ask the hospital or doctor whether there was an error or whether they wanted to correct this or so on.

Maybe I jumped too early. Because the law enforcement, the insurance company, they would love to have access—relatively free, unfettered access to records and look for lots of things. I think the question is how much access to allow people to have without having any demonstrable cause.

Dr. Palmisano a minute ago talked about kicking down the doors. Once you have things on-line, we are talking about the computer

equivalent of kicking down doors when law enforcement and insurance companies have unfettered access.

I think the standard that is common in this country in almost every State that I am familiar with is if there is probable cause, a reasonable demonstration that records have to be accessed and that can be proven to a judge, that you get a court order; and sometimes you have to make accommodations to patient privacy.

There are a couple of Federal cases that you should be aware of. The *Ariyoshi* case—

Mr. HORN. Do you want to spell that for the record?

Dr. HOGE. I think it's A-R-I-Y-O-S-H-I. It is a Hawaii State—State of Hawaii or *Attorney General of Hawaii v. Ariyoshi*, I believe, where the Medicare fraud investigation unit came in and grabbed a psychologist's records, snapped them all up. They were sealed by the judge. There was a court case that ultimately ensued, and the resolution was the court said you do have reasonable basis for looking at certain parts of this information, the billing aspects and so on, but you don't have a right to look at their private information, what the psychologist wrote about their fantasies or their fears or their personal life.

So judicial supervision of access to records or access to private information I think is ingrained in our society. We don't allow the police, even if they think there might be a crack house somewhere in the neighborhood, to go door to door and look in every house looking for it; and that may deter—may lead to some decrement in law enforcement. I am not pro-crack house, but I think we have to protect privacy, and the result of that is we have some decrement in law enforcement and fraud and abuse investigation.

Mr. HORN. Any comment you want to make on that, Dr. Palmisano?

Dr. PALMISANO. Yes, sir. The American Medical Association certainly is against fraud, but we do not want the standard for investigation lowered beyond probable cause.

The example you gave, if someone had a mastectomy 10 years ago and is being billed for it now, that should be corrected. If it was a clerical error, to determine if it's a clerical error or knowingly and intentionally done to defraud, those have to be investigated.

But when you have a reasonable belief and evidence to show that there probably is more than likely fraud going on, you can get that order to go search that information; and it ought to be limited to the information you need to search and not go through all the other information.

When individuals have the power to invade your office records or hospital records at will with a very low standard, not only is it—it is unAmerican in our opinion, but also it is very expensive. Because you have the finances of the Federal Government basically funding this, your taxpayers' money funding this. You are paying all these different lawyers to come in to advise you what to do, and it gets extremely expensive.

Mr. HORN. Well, this example, in fact, was on the information company where the doctor is sending forth the bill, lets say, where the patient has given them their health care information as to what insurance company and then the insurance company's at-

tempt to apply whatever antifraud standard is the usual procedure with that company, and the degree to which they are saying that companies would be limited in the claims investigations they could perform under H.R. 52. I don't know if they are right on that or not. Obviously, we are going to explore it.

And the question was, should there be a specific exception for claims investigations and antifraud investigation from the privacy standard which might be very high. But the whole reason you take insurance, presumably, is to get the payment. But it ought to be the accurate, truthful payment that justifies that.

Dr. PALMISANO. Well, we don't think there ought to be an exemption.

The American Medical Association, first, we are against fraud. We have helped the FBI to help root out fraud, so we are on record for that. But we think the standard ought to be kept high so they are not fishing expeditions.

Also, the approach that would solve a lot of so-called fraud problems is the approach that the American Medical Association put forward on the Worldwide Web site called Saving Medicare. It has been distributed to Congress. Basically, let the patient get more involved, let the patient get back in the driver's seat, let the patient be a fraud investigator so the patient has some responsibility in looking at the bill. The patient will know she didn't have a mastectomy and know right off the bat that is an error.

The fact of getting rid of controlling prices, get down to letting the doctors set their own conversion factors and publicize that. Then the patients and the physicians get involved and we get back to a society with less regulations. It is impossible to write regulations to cover all possible situations.

I think in terms of the heroic American effort when we were involved in the Normandy invasion after the people on the beach were killed—at Omaha beach. Ninety percent of the people that hit the beaches that day from the 116th, from Virginia, they were killed on the spot. Their ship was sunk, and they swam to shore and had to get up.

The reason we were able to get up there and knock out the machine guns—the reason we were able to knock out those big guns is because Americans were resourceful. If they had to follow some little rule book and regulation—now, if the German Army does this—they would have all been killed that day. In fact, Colonel Rudder couldn't lead the attack. The General said, "Colonel Rudder, don't do this attack;" and he said, "I am going to have to disobey you, sir. I have got to lead the men. Otherwise, it won't get done." And he did it.

That is why they say Hitler's Youth Crew lost out to the American Boy Scouts. The Boy Scouts were very resourceful.

Every time we come up with more harassment on physicians and patients, we end with a system that really doesn't work. It becomes more burdensome. So we would hope that would remain on the forefront.

Today we are talking about privacy and confidentiality, and we want to enhance that, protect that. But, on the other hand, we don't want to have rules and regulations that end up creating more burden and don't protect that.

Mr. HORN. Ms. Goldman.

Ms. GOLDMAN. My only comment to add to the ones that have been made is I think it is really important that we recognize that there should be fourth-amendment-type limits on Government access to certainly health information. H.R. 52 and the other bills that have been discussed do that. We do it to varying degrees, and the Justice Department has expressed concern about those provisions, and I am not aware that they have signed off on any of them.

I think it is a natural response on the Justice Department's part to say we now have unfettered access to personal health information. Please don't make us be bound by the fourth amendment. That is an understandable response, but it is certainly not the right one.

The fourth amendment is not an absolute bar to law enforcement access to records. What it says is, you must meet the standards, probable cause or clear and convincing standard before you can get access; and it is a protection on the individual. It is certainly not an absolute bar. And it is one, again, we see in the privacy laws we already have at the Federal level and ones that should be built into this Federal policy as well.

Mr. HORN. I must state one of the goofier implementations of privacy law in my field of education was when the Department of Education—and I happened to head a national coalition to create it, so I favored the Department—that we had strict rules written into that law that you could not impose curricula on States, et cetera. But they visited Pennsylvania State University and later California State University at Long Beach; and they said, oh, you can't display the thesis of a student in the library without the signed exception to the Buckley Act—of the privacy right.

Now only an idiot would make that kind of ruling. Unfortunately, it went up the high hierarchy. And the Secretary, when the complaint was given to him, stuck by that stupid policy.

Now the whole purpose of the dissertation and thesis is to be examined by the outside world. So here we have the case of a Federal law being used where the thesis writer could have massive plagiarism. The professors might have missed it. You can't keep up on everything in every field. That thesis is signed off, and it is normally deposited everywhere in America in the university library or the microfilm operation for dissertations in Michigan.

There is an example of people going haywire with a, quote, privacy right, unquote. There is no privacy right, it seems to me; and yet they could get away with it. They could have plagiarized; and under the Department of Education's great interpretation, they can be free because no one will ever see it. It is not on the library shelf. I don't know if they are still doing it, but they were doing that several years ago.

Ms. GOLDMAN. I would agree with you. That is an unfortunate application of a privacy law.

My experience has been a little bit different in that what I tend to see is underenforcement of existing privacy laws or weak construction of the existing privacy laws and not overzealous application. But it would be interesting to see if that is still the interpreta-

tion, because I agree with you that what is a public record ought to be available.

Mr. HORN. All right. Let us move to the next series of questions, and H.R. 52 requires health researchers to receive approval from a certified institutional review board in order to review patient records. Is that acceptable to most of you or how do you feel on that? Are there any problems with that section, which is 152 of the bill?

Ms. GOLDMAN. Well, what is interesting is that the approach taken by H.R. 52 and the one taken in last year's bill introduced by Senators Leahy and Bennett is one that at least recognizes there are Federal regulations right now that require all federally funded researchers to get the informed consent of individuals whose information may be the subject of research. So, as Dr. Gabriel said earlier, there are already requirements on federally funded researchers to have to get the informed consent, unless the IRB agrees that a waiver is appropriate and there is a standard for the waiver.

The Senate approach basically said, lets codify those regulations so that all researchers—not just federally funded researchers but all researchers will have to comply with informed consent. I think the pharmaceutical industry last year had concerns about that, but that has a fair amount of unanimity that that is a pretty good start.

I think H.R. 52, again, tries to bring in the Institutional Review Board and create another level of hierarchy, which I don't think is a bad idea, to say someone should be watching the IRBs. Because even though there has been some studies commissioned in recent months, there is no record, no factual basis to know how IRBs work as a whole, how we look at the consent mechanism, when and where they approve waiver applications. So we know little about how IRBs work. We do know they adhere to privacy issues, consider them in the application for research.

Mr. HORN. Now is there any type of research that does not require such approval?

Ms. GOLDMAN. The research that does not require approval are ones that do not involve identifiable data. And I would agree, if you are not using identifiable data, you should not have to get the consent of the records covered, because it is not within the privacy scope. Nonidentifiable data has to be clearly nonidentifiable data, and there is discussion about what that means. But I would agree that nonidentifiable data is outside the scope of a privacy bill.

Dr. ANDREWS. I would like to make a couple of comments.

First, relating to IRB review and approval—

Mr. HORN. It is Institutional Review Boards. I just want the audience to know what we are talking about.

Dr. ANDREWS [continuing]. The regulations are quite strict on IRBs. There is currently a commission that is looking at the IRB process and that, I assume, will also be looking at not only the protection of patients against medical risk but also privacy risks. There seems to be no need for additional legislation on this point which might pre-empt or prematurely set some legislation in place to pre-empt the outcome of that commission's reports.

Regarding what information is considered identifiable, I think that is a key point; and we feel that the language in the current H.R. 52 is a little too broad in identifying what would be considered personally identifiable data. For studies that use data bases that contain a key or an encrypted code that could potentially be used to link back to medical records, those studies currently do not require IRB approval or patient-informed consent. They generally are considered to fall below the level of minimal risk that would determine the need to have informed consent.

In addition, as you have also heard from Dr. Gabriel, informed consent is frequently not feasible in these circumstances in using very large data bases answering questions that may arise many years after the information was collected, because there is difficulty locating patients in our highly mobile society, getting consent itself may introduce a bias, and because contacting patients may also constitute a violation of patient privacy.

In addition, as you have also already heard, if you use only the patient data from those who have been located and provided consent, you may introduce a bias in the study which may invalidate the study findings.

Mr. HORN. Dr. Hoge has a comment.

Dr. HOGE. Actually, yes, and maybe in the way of a question. I am a little unclear if a doctor enters in the data base that you are talking about has a code, could be stripped of that code.

I guess the point I am asking, it seems it would be reasonable to ask IRB approval if there is going to be the future capacity to relink that code to the person's actual identity, because now you have got a privacy concern that someone should be overseeing. But if you are going to take the information, strip it, it doesn't seem to be a problem, but maybe I am misunderstanding.

Dr. ANDREWS. I think there is something in between that. I believe that data bases totally stripped of identifiers should be excluded. Then there are data bases that have an encrypted code that could be linked back, and we also feel those should be exempted.

I think the actual relinking, which I think is what you are referring to—someone is taking the code, relinking, identifying patients and abstracting additional information to supplement the original study; and those do need very tight security over the relinking and may need and usually are, I believe, covered by IRB review and approval at the moment.

Dr. HOGE. If I might—but, again, if there is a potential to relink through the code, that means you either have the plan or some expectation of relinking it; and, therefore, there is some privacy risk—I don't understand. It seems a little disingenuous. If you are not planning on relinking, why don't you just strip it? And if you are planning to relink it, it seems to me you are back at a point where you have got to get IRB.

Mr. HORN. Do you want to respond to that, Dr. Andrews?

Dr. ANDREWS. The reality is these data bases often have been so carefully developed that this encrypted code is available for the researcher. The researcher cannot by themselves identify the patient, and they have no interest in doing so. They are interested in the aggregate data. It is the local physician or a third party that would be able to take that encrypted code and link back.

Mr. HORN. Dr. Gabriel.

Dr. GABRIEL. I just wanted to make the point that all of the research that I mentioned in my statement is already covered by the IRB. In fact, at our IRB we apply the regulations to everything, federally funded or not. So I would endorse having the IRB approval for all of these studies.

Mr. HORN. Dr. Palmisano.

Dr. PALMISANO. Thank you, Mr. Chairman.

I just wanted to emphasize that when we put in the statement—both oral statement and written statement—that medical information used for research purposes should have all identifying information removed unless a patient specifically consents to the use of his or her personally identifiable information; and on the subject of research it can be a troublesome category of exceptions to the general requirement for patient consent. Although in conclusion, we are generally satisfied that the IRB patient protections are adequate, we believe that a scientist should be able to pursue legitimate research without unreasonable barriers and that it is possible to do this while still protecting patients' privacy. What we don't want to see is the term research applied to a whole spectrum of economic analysis that solely benefits shareholders rather than patients.

I guess I would like to pose a question back on H.R. 52. On page 39, it states that the project has been determined by a certified Institutional Review Board to be of sufficient importance to outweigh the intrusion into the privacy of the protected individual who is the subject of the information that will result from the disclosure. So it appears from this reading that privacy will be invaded, and the IRB is saying that the research is of sufficient importance. So it is not being treated as an IRB study.

Consultation is being obtained with the IRB to decide whether or not it is of sufficient merit to invade privacy, and what we say is that medical information used for research purposes should have all identifying information removed unless a patient voluntarily and knowingly and willingly consents to that information.

So it is right to go through the Institutional Review Board. We think—a lot of them we hold in high regard.

On the other hand, we don't know that this is going to protect the privacy—it goes back to the philosophical discussion, is the teleological approach to the philosophical base whereby you say, well, the end justifies the means, so we are going to invade privacy to do this research and find out these potentially good things. We think the patient's privacy must be paramount.

Thank you.

Mr. HORN. Dr. Gabriel.

Dr. GABRIEL. I wanted to respond to that a little bit.

As we said before, the researcher is not aware that this is Mrs. Jones' data. The only place that privacy might be invaded—there has to be a point somewhere where you collect the data from the medical records, put it in a data base, strip the identifiers, and that is where the analysis happens.

So I have a question. How do you define nonidentifiable data? There has to be—so the point, at least in the way we do things, we have usually a nurse administrator abstract a piece of information from a medical record and then that is put in a data base with

hundreds of other people's data and then the information or the patient identifiers are removed. So when you were reading that I was thinking maybe that was what they were referring to.

Dr. PALMISANO. Mr. Chairman, it is just a question. I am not sure what is being referred to. I think it is vague as written here. It may be because of my ignorance, I don't know, but I would like it clarified.

I certainly understand how I could see a scenario. I don't consider myself a computer wizard, but I would see where you could send someone who understood confidentiality and taken an oath, could go to medical records and say, all names will be removed and codes will go in there and these codes don't necessarily link up, but it identifies whatever you need to identify without identifying the individual and that would be given to the researcher. It appears from what I have heard that would satisfy the researcher.

So I think that could be done from a technological basis, and those who are much smarter than I am in computer methodology could come up with an even better way than that. But it appears that the information could be interpreted by a reasonable individual to say that we are going to allow the name to be kept with this record because the research is of such moment that the IRB, they agree, is really of great moment. So they have this invasion of privacy without the individual knowing; and the individual may say, no, I did not want you to allow that. I did not want to take the risk, however small, 10th of 1 percent that it would be discovered by someone else.

Mr. HORN. Perhaps we should have staff talk to the National Institutes of Health. Because you could have a project that takes 5 to 10 years, maybe, to come to some conclusion; and the question is, if you do discover something that relates to that sample or you want a later subsample of that, is there a way you can tie that back to the good of the patient?

Yes, Dr. Andrews.

Dr. ANDREWS. Let me address this question of relinkage.

While I may strip a data set, there are some circumstances where you would want to have the ability to go back and relink; for example, if you are doing a study on the safety of a particular kind of drug and you may follow patients for 6 months. If you obtain a signal that this drug may be causing cancer and the latency period is longer than 6 months, then you might want to use that same cohort of patients, extended for a longer period of time, in which case you need to take the data set back to its origin, relink through a very careful time-limited linkage, and gather the information that would then go into the data base that would no longer have the identity. It would be that linkage process that would need to be carefully safeguarded, rather than the whole data base. So I think we are all saying the same thing.

[The information referred to follows:]

## Informed Consent As Contract: *Dahl v. Hem Pharmaceuticals Corporation*

by John M. Isidor, Esq.

*John M. Isidor, Esq. is an attorney in private practice and vice chairman of Schulman Associates Institutional Review Board, Inc., an independent Institutional Review Board in Cincinnati. Since becoming involved in clinical research through his affiliation with Schulman Associates, Mr. Isidor has become a frequent lecturer on how legal and regulatory issues affect the conduct of clinical trials.*

Clinical trial sponsors should pay particular attention to a recent U.S. Court of Appeals decision that an informed consent document was a contract that required a sponsor to perform services for study subjects even after the clinical trial ended. The case also recognized the right of study subjects to bring suit against a sponsor to prevent the termination of their participation in the study. The decision also is significant because it held that under certain circumstances clinical investigators could be found to be the agents of the sponsor.

Examining the facts of this case brings to the surface many potential problems for sponsors, including contractual performance obligations produced by consent documents, and limitations on sponsors' rights to terminate a study.

In the unprecedented case, *Dahl v. Hem Pharmaceuticals Corporation* (Dahl), 7 F.3d 1399 (9th Cir. 1993), the U.S. Court of Appeals for the Ninth Circuit reached some startling conclusions in responding to contractual claims made by a group of subjects participating in the clinical trial of the drug Ampligen, used for the treatment of chronic fatigue syndrome (see p. 9 for decision).

In *Dahl*, Kristina Dahl and 17 other clinical subjects sued Hem Pharmaceuticals Corp., alleging that the terms of their informed consent documents obligated the company to continue to provide them with study medication after the conclusion of the study (see ¶¶430-436).

Based on the unusual circumstances in the case, the Ninth Circuit Court of Appeals affirmed the 1991 decision of the trial court: The informed consent document was a legally binding contract which obligated Hem Pharmaceuticals to continue providing Ampligen to Dahl and the other subjects for 12 months after their participation in the study ended. The trial court also found that by signing the consent

document on behalf of the sponsor, the investigator acted as the legal agent of the sponsor and was capable of binding the sponsor to all the terms contained in the document.

### Background

In October 1990, Hem Pharmaceuticals conducted a study on the investigational drug Ampligen. According to the terms of the protocol, patients would be administered the drug or a placebo twice per week for a maximum of 12 months (see ¶510).

On March 22, 1991, Hem filed an amended protocol with the FDA reducing the time period of the double-blind phase from 12 months to six months (see ¶321). This amendment also stated that following the double-blind phase, Hem would provide an open-label phase for participants who exhibited a substantial response to the study medication as determined by the sponsor. Further, the amendment provided that participants who did not exhibit a substantial response to the medication would be removed from the study at the end of the double-blind phase. When Ampligen's efficacy was established, those participants would be enrolled in the open-label phase on the same basis as the participants who exhibited substantial responses.

On April 4, 1991, Hem submitted a second amended protocol, increasing the frequency of dosages during the double-blind phase from two times per week to three times per week. Subsequently, believing Ampligen to be more effective than the placebo, Hem submitted a treatment Investigational New Drug (IND) application to the Food and Drug Administration (FDA).

Dahl's participation in the study began on April 8, 1991, several days after the submission of the second amended protocol. During the double-blind phase of the study, Dahl exhibited substantial responses and began receiving Ampligen under the open-label phase.

On Oct. 4, 1991, the FDA issued a letter informing Hem that they could not proceed with their treatment IND and placed the program on clinical hold (see ¶1151). However, the FDA allowed the open-label study of Ampligen to continue.

#### Dahl's Informed Consent

Dahl, who is a physician, alleged that she was permitted to begin treatment with Ampligen before signing an informed consent document (see ¶434). Several weeks after she began treatment, Dahl was given an informed consent document by the site coordinator, who already had signed the document on behalf of either the investigator or the sponsor (see ¶434). Although asked to do so, Dahl did not sign the informed consent document. In preparation for an impending FDA inspection five months later, the site coordinator noticed that Dahl was the only participant who had not signed a consent form, and again asked her to sign the document. On Sept. 16, 1991, she did so.

However, Dahl did not sign the form as presented; she made several alterations. First, where the form stated that she would participate in a double-blind study lasting a maximum of 24 weeks, Dahl crossed out the reference to 24 weeks and instead inserted "12 month." The form also stated that if, after six months, statistics showed Ampligen to be effective as compared to the placebo,

**"Dahl did not sign the forms as presented; she made several alterations."**

Dahl would receive Ampligen, but it did not specify the length of time for which she would receive the drug. So, Dahl added the phrase "for 12 months" to that statement. Although the form did not

specify whether or not Dahl would be charged for Ampligen should she receive it after the end of the double-blind phase, Dahl added the words "without charge."

Finally, while the form stated that Dahl would receive Ampligen injections twice a week for the first four weeks of the study, and three times a week for the remainder of the study, Dahl changed the form to read that she would receive Ampligen injections three times a week for the entire duration of the study. Dahl returned the altered informed consent document to the site coordinator and continued to receive Ampligen or placebo injections until concluding the open-label phase of the double-blind study.

Dahl and the other plaintiffs filed suit against Hem Pharmaceuticals when Hem ceased to provide Ampligen at the end of the study. They asked the court to require Hem to continue providing Ampligen for another 12 months at no cost to the subjects (7 F.3d at 1404). Both the trial court and the Court of Appeals granted the relief requested by the plaintiffs.

#### Informed Consent Document: A Contract?

The trial court and the Court of Appeals found that the informed consent document was a contract committing the sponsor to the performance described in the form. Hem Pharmaceuticals tried to convince the court that because the subjects participated voluntarily (see ¶433) and were free to withdraw at any time, they had not entered into a contract (7 F.3d at 1404). However, the Court of Appeals rejected that argument, ruling that by completing the double-blind phase of the study, the subjects created a binding contract which obligated Hem to provide a year's treatment with Ampligen at no cost to the subjects.

Under general contract law, both parties to a contract obligate themselves to some specified type of performance. Hem argued that the clinical trial subjects were not parties to a valid contract because they had not incurred any detriment or obligated themselves to the contract. The Court of Appeals again disagreed, ruling that the subjects' commitment to the contract was evidenced by the fact that they had submitted themselves to months of injections with either Ampligen or the placebo, as well as other intrusive and uncomfortable testing procedures required of all study participants.

#### Investigator as Sponsor's Agent

During the trial, Dahl and the other plaintiffs argued that the site coordinator and the investigator acted as agents of Hem Pharmaceuticals, thereby obligating Hem to the performance promised in the informed consent document. The trial court agreed, finding that the site coordinator acted as the sponsor's agent by presenting the informed consent document prepared by the sponsor to Dahl, as well as by signing the document on behalf of the sponsor.

When the sponsor argued that the investigator was not an agent, but rather an independent contractor, the trial court sided with Dahl and found the investigator

to be the sponsor's agent. Although the contract between the sponsor and the investigator stated that the investigator was an independent contractor and not an employee of the sponsor, the court nevertheless found that the sponsor had the right to direct or control the services provided by the investigator, including the right to fire the investigator if he did not comply with the terms of the protocol (21 CFR §312.56(b), see App. II). Based on these findings, the court determined that the investigator was the agent of Hem Pharmaceuticals.

#### Future Implications

The determination of the court that the informed consent document is a contract between the subject and the sponsor has many ramifications for clinical trial sponsors. Of greatest concern is the concept that the informed consent document can obligate the sponsor to perform such services as continuing to provide study medication to the subjects after the study ends. Furthermore, the decision appears to limit the rights of the sponsor to terminate the subject from the study or to cancel the study. Additionally, the case recognized the right of subjects to file suit to prevent cancellation of the study or termination of their participation in the study.

Because the subject's right to sue – under the theory that the informed consent document is a contract – has been recognized (at least in those states located within the jurisdiction of the Ninth Circuit Court of Appeals), language in the informed consent document that can be interpreted to mean that the subject waives any rights he or she may have could violate the federal regulations on informed consent. These regulations state:

"No informed consent, whether oral or written, may include any exculpatory language through which the subject or the representative is made to waive any of the subject's legal rights ..." (21 CFR §50.20, see App. II).

An example of a potential violation of this regulation would be a clause in an informed consent document stating that the document is not to be considered a legal contract.

In addition, the court's determination that the document is a contract stresses the need for clear and precise drafting to specify the obligations of the sponsor and the investigator. This is necessary because as a matter of traditional contract law, any ambiguity in a

contract is interpreted against the party who drafted the contract.

The peculiar course of events leading up to Dahl's alteration of the informed consent document – after signature on behalf of the sponsor – highlights the im-

portance of following the proper procedures when having subjects sign forms (see ¶434). Those responsible for monitoring a study carefully should review the forms to make certain that prior to participating in the study, the subject has signed all forms as presented, or, if altered, that the alterations are acceptable to the sponsor (*FDA Guidelines for the Monitoring of Clinical Investigations*, see App. III).

The court's determination that the investigator is the agent of the sponsor also is troubling, because it suggests that the sponsor can be found responsible for the actions of the investigator, such as the investigator's failure to provide informed consent. This holding contradicts traditional informed consent law that only a physician, and not a pharmaceutical company, can be found liable for failure to provide informed consent.

In *Tracy v. Merrell Dow Pharmaceuticals*, (Tracy) 58 Ohio St. 3d 147 (1991), the Ohio Supreme Court considered whether an investigator in a clinical trial is an independent contractor. Contrary to the finding of the court in *Dahl*, the Ohio Supreme Court determined that the investigator was an independent agent because he exercised his own independent judgment in determining the eligibility standards for the study and for monitoring the subject's course of treatment (58 Ohio St. 3d at 150-51). The *Dahl* decision demonstrates a worrisome interpretation of similar facts that raises the spectre of new types of liability for sponsors.

Finally, the sponsor may lose the learned intermediary defense, one of its best defenses to a product liability lawsuit for the failure of the investigator to warn the study subject of the potential dangers of a product. This defense historically has relieved sponsors of the liability to a subject if they fully inform the investigator, who is considered to be a learned intermediary, of the risks involved in the use of the drug. As the learned intermediary, the investigator is

**"The determination that the informed document is a contract ... has many ramifications for clinical trial sponsors."**

delegated the responsibility of warning the subject of any risks involved, because he has the opportunity to evaluate the subject and to supervise the use of the product.

In *Tracy*, the Ohio Supreme Court determined that since the clinical trial investigator acted as an independent physician when dispensing the medication, he was a learned intermediary thereby shielding the sponsor from liability for failure to warn the subject of the risks of taking the study medication (58 Ohio St. 3d at 151). However, by employing the reasoning of the court in *Dahl* that the investigator was the sponsor's agent, the learned intermediary defense could fail in future product liability cases.

***"As the learned intermediary, the investigator is delegated the responsibility of warning the subject of any risks involved ..."***

The court's finding that the investigator is the sponsor's agent creates a potential dilemma for the

sponsor. If the sponsor drafts the informed consent document, of course the sponsor is responsible for everything it promises to do for the subject. Yet, under the holding in *Dahl*, even if the investigator drafts the informed consent document, the sponsor still will be held responsible for all the promises contained in the document, including an ambiguous or open-ended compensation for injury clause. The *Dahl* decision demonstrates a need for sponsors to monitor the contents of informed consent documents, regardless of whether or not the drafter is the sponsor or the investigator.

#### Conclusion

While the issue of informed consent as contract was theoretical before, *Dahl* creates legal precedent, at least in one area of the country. It gives research subjects in clinical trials new remedies under contract law when a sponsor seeks to cancel or terminate a subject's participation in a study. Further, the *Dahl* opinion highlights the necessity for careful sponsor and investigator monitoring of the informed consent process. ♦

Ms. GOLDMAN. I have to add one thing on the research.

I think there is a fair amount of agreement the vast amount of research that is done in this country is done with the deidentified data, out the personal identifiers. For that small group of research that is done with identifiers, I again say that it is very important that informed consent of patients be obtained. Because, as a few people have testified, there is a concern about there being a bias, that those that opt out would create a bias. At least it is a known bias.

You know, there are a small group of people who say, I am uncomfortable being a part of this research project because I am concerned with confidentiality or I am concerned about losing my job or whatever it is, which are real concerns on the part of the individual.

The current situation we have, where identifiable data is used in research without individuals' consents, the bias in those research projects involve people who give inaccurate information because they are afraid of the lack of privacy. People who lie, people who don't seek treatment, those create biases; but we don't know about them. We can't quantify them. At least—if they opt out and the information is asked for and it is withheld, at least you know who is saying I do not want to be a part of this research project.

Mr. HORN. Well, that leads to the next question. If some patients are willing to give general waivers at the outset of their treatment permitting future disclosures of records to providers, researchers and others, should H.R. 52 prevent that or should each research project require informed consent of the patient to be sampled at that particular time?

Ms. GOLDMAN. The way H.R. 52 is written is in authorization there has to be an identification of who the recipients would be and what the information would be used for.

If the authorization is written broadly enough—and, again, getting that authorization does not then condition whether or not you deliver benefits or services. If people want to be part of ongoing research and that research is specified, it is not my judgment to make. I think these are individual judgments that people should make.

The beauty of the privacy law that is crafted like this, it lets people make those choices. It lets doctors talk to the patients and say, I would like you to be involved with this; I think it would benefit you. It allows researchers to come in and have contact with people and talk to them about the benefits and risk. That is what is allowed here. It allows people to make their own choices and not myself or anyone else in this room to say here is the standard, here is what should apply.

Mr. HORN. OK. We are going to wind this up.

Anything any of you have on your mind that we haven't asked about in this hearing record?

Dr. HOGE. I think you were a born therapist.

Mr. HORN. We don't get those wages—sorry—salary, whatever, bills paid.

OK, I want to thank you all very much for coming. You have all raised some new questions, as any good hearing does; and we will be following up. Just like your comments, as we go, if there is a

new draft bill put together, we will send them to you. We would like your comments. Those of your association would be very helpful.

With that, this hearing is adjourned.

Oh, let me just put the staff on the record. I want to thank the following people that worked on this.

J. Russell George, the staff director and chief counsel; and Mark Uncapher, who is on my left, your right, the counsel for this hearing; John Hynes, professional staff member; Andrea Miller, clerk. David McMillen, professional staff member for the minority; Ron Strohman, professional staff member for the minority; Jean Gosa, clerk for the minority; and Sheridan Parker, minority research assistant.

We have had interns with this particular hearing: Mike Pressicci, Grant Newman, Melissa Holder; and our court reporters are Katrina Wright and Tracy Petty.

Now we are adjourned.

[Whereupon, at 12:30 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Mr. Chairman, on behalf of the members of the National Association of Chain Drug Stores (NACDS), thank you for the opportunity to present testimony to the Government Management, Information and Technology Subcommittee regarding the *Fair Health Information Practices Act of 1997* (H.R. 52), introduced by Congressman Gary Condit (D-CA). We applaud your leadership in holding hearings on this important topic.

Founded in 1933 and based in Alexandria, Virginia, the NACDS membership consists of more than 130 retail chain community pharmacy companies. Collectively, chain community pharmacy comprises the largest component of pharmacy practice with over 86,000 pharmacists. Chain community pharmacy is comprised of 18,500 traditional chain drug stores, over 6,000 supermarket pharmacies and nearly 5,000 mass merchant pharmacies. The NACDS membership base operates nearly 30,000 retail community pharmacies with annual sales totaling over \$110 billion, including prescription drugs, over-the-counter (OTC) medications and health and beauty aids (HBA). Chain operated community retail pharmacies filled approximately 60% of the more than 2.5 billion prescriptions dispensed annually in the United States. Additionally, NACDS membership includes more than 1,250 suppliers of goods and services to chain community pharmacies. NACDS international membership has grown to include 67 members from 22 foreign countries.

#### **Patient Confidentiality Requirements Must be Uniform Across State Lines**

Preserving patient confidentiality is an essential part of the day-to-day operations of a community retail pharmacy. Today, virtually all pharmacy patient records are maintained electronically. Licensed pharmacists must abide by the many different state patient confidentiality standards specified in state pharmacy practice acts, state board of pharmacy regulations, and other state laws. In addition to these many requirements, community retail pharmacies commonly include stringent patient confidentiality policies for their employees.

NACDS cannot support the enactment of H.R. 52 as currently written, or any other federal health care confidentiality bill that does not preempt state health care confidentiality laws because community retail pharmacies will have trouble complying with multiple and possibly conflicting requirements across state lines.

H.R. 52 does not preempt state health care confidentiality laws, but instead cites many state exemptions to this federal legislation. Community retail pharmacies may not be able to comply with a federal confidentiality law that does not preempt state law, because it would be nearly impossible and economically infeasible to program computer software prompts for the multiple requirements and exemptions resulting from adding new federal law to the growing body of state patient confidentiality law. In effect, this legislation would add even more requirements and increase, rather than decrease, the different and sometimes conflicting combinations of law multistate providers must follow.

When the federal law is a floor, rather than a ceiling, every state exemption increases the amount of information that would have to be considered in the development of compliance software for pharmacies. In light of the highly computerized pharmacy environment, this type of software would be essential to prompt health care providers on specific compliance requirements. Without such software, community retail pharmacists would have to be trained to manually decide, provision by provision, whether the federal or state law is more stringent... all while the patient is waiting for a prescription. This presents an impossible compliance situation.

H.R. 52, like many of the other federal health information privacy bills, seems to be written for the institutional health care provider with a large administrative support staff. Indeed, compliance with the many and complex requirements of H.R. 52 and other bills would require a health care provider to have a large administrative staff. Community retail pharmacies rely on the efficiencies of complex computerized records systems specifically to avoid expensive administrative burdens. Congress must write legislation so that compliance doesn't impose an onerous and expensive administrative burden for community retail pharmacies and small businesses.

H.R. 52 was drafted with a recognition that serious implementation problems are likely to arise and creates the Office of Information Privacy to help solve these problems. NACDS believes this is the wrong approach. H.R. 52 could increase health care provider costs and subject providers to needless criminal and civil suits. Therefore, implementation problems must be addressed before the bill is enacted. Hearings should be used to gather information about implementation problems and demonstration projects should be considered prior to the enactment of comprehensive patient confidentiality legislation. Patient confidentiality legislation must be done right the first time rather than being treated as a work in progress... the costs are simply too great to do it any other way.

Any federal health care confidentiality legislation must be streamlined as much as possible to make compliance as easy as possible. Community retail pharmacies frequently dispense a patient's prescription(s) while a sick patient waits in the pharmacy. Patients' waiting time will be needlessly extended if federal privacy legislation requirements are not streamlined to accommodate this patient service environment.

#### **What NACDS Does Support**

*NACDS Principles for Safeguarding Patient Confidentiality* set forth below clearly describes what NACDS would support in federal health care confidentiality legislation:

- Stiff penalties and fines for those who knowingly breach the confidentiality of patient records.
- Provisions to discourage any unauthorized, inappropriate use of confidential information, including any use for personal gain or personal profit.

- Provisions to allow the necessary interchange of patient-identifiable information among health care providers, such as physicians and pharmacists, and to ensure the most effective and efficient delivery of the highest quality health care services.
- Comprehensive and stringent standards so that state patient confidentiality laws are unnecessary. Community retail pharmacies, especially those that operate in multiple states, will operate most effectively with one federal set of confidentiality standards.
- Retention of state pharmacy practice acts and state board of pharmacy regulations concerning the definition of the practice of pharmacy and the requirements of who may practice pharmacy in the state.
- Requirements for the public sector to work together with ANSI accredited standard development organizations, such as the National Council of Prescription Drug Programs, to establish standards for the safeguarding of electronic transmission, storage, and validation of patient information.
- A thorough analysis of the overall financial impact of federal confidentiality standards on health care industries and professions, including community pharmacies.
- A realistic time-frame to implement new uniform confidentiality standards, including time for software and hardware development, testing and distributing of these products, and health care professional training on these products. Retail pharmacy would require a minimum of 18 months to implement regulations once they are promulgated to allow for the development of and training on new software and the purchase of hardware.

**Conclusion**

The NACDS looks forward to continuing to work with this panel in the future on federal confidentiality requirements that will allow providers to continue providing quality health care services with as little inconvenience to patients as possible. Again, we appreciate the opportunity to testify on this important issue before the Subcommittee.

**Written Statement  
of  
John T. Nielsen, Esq.  
Senior Counsel  
and  
Director of Governmental Affairs  
INTERMOUNTAIN HEALTH CARE**

**before the**

**House Government Reform and Oversight  
Subcommittee on Government Management,  
Information, and Technology**

**Hearing on H.R. 52  
the "Fair Health Information Practices Act of 1997"**

**June 5, 1997**

Intermountain Health Care, Inc. ("IHC") is a large integrated health care system based in Salt Lake City, Utah, consisting of 23 hospitals, 33 clinics, 16 home health agencies, 300 employed physicians, and IHC Health Plans which is a mixed model HMO with an enrollment of 350,000 members including Medicare and Medicaid beneficiaries in Utah, Wyoming, and Idaho. IHC is pleased to submit its comments on medical records confidentiality.

IHC has spent significant time and effort in addressing the issues surrounding the appropriate use of medical records information. Already, IHC has twice testified before the National Committee on Vital and Health Statistics (NCVHS) on health confidentiality

issues (*see* attached copy of our most recent testimony before NCVHS, which was presented February 18, 1997 on behalf of the American Hospital Association.)

IHC supports this Subcommittee's efforts to protect against the unauthorized and inappropriate use of patient information while at the same time facilitating the coordination and delivery of high quality, network-based health care. IHC looks forward to working constructively with the Subcommittee on this important issue. Use of medical records information is critical to our delivery system's operations and efforts to improve our members' health outcomes.

Unique Needs of Network-Based Care

IHC urges the Subcommittee to recognize the special needs of large integrated health care delivery systems, such as IHC. Network-based care relies on the coordination of patient care by providers and effective quality enhancing activities which include: quality assurance programs; data analysis for disease management activities; outcomes research on safety, efficacy, cost-effectiveness, and quality of life, accreditation and certification activities; and provider screening and profiling.

Many of these activities require the use of individually identifiable information. Moreover, even in cases where nonidentifiable information can be used, health plans must be able to link the nonidentifiable information back to a specific individual in the event that a more effective treatment protocol or a previously unknown health risk is identified.

For example, a measure of IHC's efforts to improve clinical and service quality centers on the development of Care Process Models or practice guidelines. In developing Care Process Models for chronic conditions such as asthma and diabetes, individual patient information is used to identify members at risk of complications or who are not receiving care consistent with the best care guidelines. IHC and our network of multi-disciplined providers need this information in order to reach out and communicate directly with those patients and their primary care physicians concerning the patients' profile of care and use of medical services.

As an integrated delivery system, IHC is responsible for the health outcomes of the patients who seek care from our system. In order to manage and improve the health outcomes of the population we insure, we must be able to share information among IHC corporate entities -- our physicians, hospitals, and health plans. IHC has developed electronic medical records and common databases to facilitate this communication. **Preventing the creation of these common databases, limiting the type of data which**

**could be shared within the IHC integrated delivery system and requiring a patient's authorization for each and every transaction and transfer of data would severely impede IHC's ability to measure and improve the health outcomes of its enrollees.**

IHC Patient Confidentiality Efforts

IHC has invested in many efforts to ensure security and confidentiality of health information. Included in these efforts are:

- ◆ The development of an IHC Employee Confidentiality Agreement;
- ◆ Consequences for improper use or handling of confidential information;
- ◆ Access to patient information by "need to know" and by job description;
- ◆ Software controls including warnings on front log-on screens, unique log-on passwords, and computerized audit trails; and
- ◆ A pro-active stance in the development of local and national confidentiality policy.

All health systems should be encouraged to adopt measures such as these to minimize the likelihood of inappropriate disclosure of sensitive clinical information.

Federal Preemption of State Law

If health care systems are to build an information infrastructure, it is imperative that we, as a society, develop federal standards that address these privacy concerns. Current state laws and regulations governing the exchange of patient information are often

barriers to this development and, because of their inconsistency, confusing. Many state and federal laws create obstacles to legitimate sharing of health information that could yield better patient care, administrative savings, and more efficient patient management. For example, some states prohibit the use of computerized record systems by requiring that orders be written in ink, often referred to as the "quill pen" laws, or by mandating that health record storage be restricted to the original paper or microfilm.

Moreover, payers and providers that operate in more than one state are required to comply with a multitude of different rules, which adds to administrative inefficiency. The burdensome and costly obligation of complying with individual--and often inconsistent--state laws is obvious. Such costs add nothing to the quality of care and divert resources that could be better deployed.

A uniform federal law is an important step in ensuring that individually identifiable health care information is maintained confidentially as it travels from place to place--including across state lines. Accordingly, IHC supports federal preemption in any law dealing with these issues.

### **Conclusion**

IHC has taken a pro-active stance in the continuous development of local and national confidentiality policy as well as improvements to our own internal systems. We

remain acutely aware of our responsibility to protect individually identifiable health care information and to safeguard against inappropriate use.

Because the use of medical records information is critical to maximizing patient health, great care must be taken in fashioning a legislative solution that will allow health care information to move appropriately between providers, while ensuring privacy and confidentiality. IHC appreciates this opportunity to present its views and looks forward to working with the Subcommittee.

**FOR THE RECORD**



**Statement  
by the American Hospital Association  
to the  
Subcommittee on Government Management,  
Information and Technology  
Government Reform and Oversight Committee**

**RE: Medical Records Privacy, H.R. 52**

**June 19, 1997**

The American Hospital Association (AHA), representing the nation's 5,000 hospitals, health care systems, networks and other providers of care, appreciates this opportunity to present our views on H.R. 52, the Fair Health Information Practices Act of 1997, introduced by Representative Gary Condit (D-CA). AHA members care for patients on a daily basis, and as a result, they are heavily involved in both using protected health information and in ensuring the privacy of that information. Our comments reflect members' experiences in balancing these two important goals.

**Environmental Overview**

This country's health care delivery system continues to move toward integrated networks of providers. As we seek to control health care spending, more and more communities are finding

Washington, DC Center for Public Affairs  
Chicago, Illinois Center for Health Care Leadership  
Liberty Place, Suite 700  
325 Seventh Street, N.W.  
Washington, DC 20004-2802  
(202) 638-1100

workable solutions by integrating medical services and financing. These community-based health networks have incentives to actively manage patient care and the potential to yield more efficient and appropriate utilization of health care resources.

Central to an integrated delivery system is a health information infrastructure. Providers need patient information to move smoothly across time, sites and providers of care to realize a more effective coordination of care. For example, a community-based network can use individually identifiable health information to develop a database that locates patients at risk of complications or disease, but who are not receiving care consistent with best-care guidelines. This can, for example, mean contacting women over 50 who have not received a mammogram, or contacting diabetic patients who have not had an annual eye exam.

In addition, selected data from such a system, when properly authorized and protected, is useful to other health information users, such as health care managers, payers, purchasers, and researchers. However, because these users are not directly involved in the treatment of patients, much thought should be given to the extent of their need for individually identifiable information.

Our challenge is to find an acceptable balance between providing appropriate access to health care information and protecting a patient's right to privacy. If health care systems are to build an information infrastructure, it is imperative that we, as a society, develop federal standards that

address these confidentiality concerns while ensuring that these standards are not burdensome and do not delay necessary care.

The AHA believes that to be effective, confidentiality standards must be uniform and offer a high level of patient protection. Currently, many state laws do not address a patient's right to see and copy his or her own medical records. In addition, many state laws and regulations create obstacles to the legitimate sharing of health information that could otherwise yield better patient care, administrative savings and more efficient patient management. For example, payers and providers operating in more than one state are required to comply with a multitude of different rules which adds to administrative inefficiency. Also, some states prohibit the use of computerized records systems by requiring that orders be written in ink (often referred to as the "quill pen" laws), or by mandating that health record storage be restricted to original paper or microfilm.

Because many of these state laws are written in the context of the paper records of yesterday, they frequently do not offer sufficient security in today's world of electronic data interchange. Many state laws do not address the obligations of anyone who comes in contact with individually identifiable health information -- including but not limited to payers, providers, processing vendors, and utilization review organizations -- to protect confidentiality. The shared information networks of the future will require uniform confidentiality requirements for handling individually identifiable health care information. Therefore, a uniform federal law is an

important step in ensuring that this information is maintained confidentially as it travels from place to place -- including across state lines.

### **Legislation**

We must exercise great caution in drafting legislation to ensure that patients receive the care they need when they need it and preserves their privacy in the process.

The AHA believes that H.R. 52 contains elements of a good medical records confidentiality proposal. However, the bill would be difficult to implement because it attempts to anticipate and categorize every use and user of health information. This is an impossible task. Inevitably, some important users and uses of information will be omitted. For example, by identifying specifically who qualifies as a "health information trustee," the bill does not apply to any entity other than those listed in H.R. 52. The bill should apply to anyone or any entity who has access to or uses individually identifiable health information, whether they are typical users of health information -- listed "trustees" -- or not. Legislation addressing a patient's confidentiality must establish standards that will apply to all potential users and must be written broadly enough to apply in all applicable situations.

While we have some concerns over the general approach of H.R. 52, the AHA does agree with the principles the legislation is built on and some of the policy contained within it. Specifically, the legislation:

- Preempts state confidentiality laws. The legislation ensures that patients are guaranteed certain confidentiality protections regardless of the state they live in. This level of uniformity also addresses the concerns of health systems that operate in several states. However, we are concerned that the exception for states to have more stringent requirements for their own agencies may create confusion over the standards in those states, and believe it warrants further discussion.
- Requires anyone who has access to individually identifiable data to establish appropriate internal safeguards to protect that information. As health care delivery becomes more integrated, confidentiality within systems becomes even more crucial.

While H.R. 52 appropriately stresses the need for internal safeguards, the AHA is concerned that the legislation does not define how the concept of "internal" would be applied to the movement of information within systems of care. In fact, there is no definition or specific provision addressing delivery systems that coordinate care. The definition of provider seems limited to individual providers and does not appear to include groups of providers. This is particularly problematic in the area of authorizations. As written, H.R. 52 could require each person within a system to seek authorization to move information to others who need it to treat the patient. Given that a multitude of persons and departments are often involved in even the most routine care, this would need to be clarified.

- Gives patients the right to review and copy their own medical records. AHA supports this important new federal protection for patients.

- Establishes civil and criminal penalties for the disclosure of individually identifiable information. Penalties should be stringent enough to act as a deterrent, but not punish users for inadvertent unauthorized disclosures. The AHA supports matching the level of the sanction to the level of the violation.

However, we are concerned that the private right of action does not include the proviso that the individual show that harm was done, and does not include the ability for information users to defend themselves on the basis that they made a good faith effort to obey the law and prevent the unauthorized disclosure.

- Includes the concept that individually identifiable information should be encrypted at the earliest possible point. While the bill discusses this in the context of research, it could be expanded into areas such as: utilization management, some quality assurance functions, certification, etc. The AHA agrees with Representative Condit that this area should be explored further as a mechanism for protecting patients' privacy.

#### **Conclusion**

In the modern health care system, many health care providers will either deliver care or share information about care across multiple jurisdictions. To protect unauthorized disclosures of individually identifiable health care information and preserve privacy and confidentiality, comprehensive federal legislation must be enacted that will ensure uniform and confidential

treatment of this data. However, there must be a balance between the necessary flow of health information for clinical and administrative purposes and the protection of patients' rights.

We appreciate the opportunity to present our views. The AHA looks forward to working with the subcommittee and the Congress to enact appropriate confidentiality legislation.



**American Council of Life Insurance**

**STATEMENT  
OF  
THE AMERICAN COUNCIL OF LIFE INSURANCE  
SUBMITTED  
TO  
THE HOUSE GOVERNMENT REFORM AND OVERSIGHT SUBCOMMITTEE  
ON  
GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY  
REGARDING  
MEDICAL RECORD CONFIDENTIALITY  
AND  
THE FAIR HEALTH INFORMATION PRACTICES ACT OF 1997 (H.R. 52)**

The American Council of Life Insurance (ACLI) is pleased to submit to the House Government Reform and Oversight Subcommittee on Government Management, Information, and Technology our comments on medical record confidentiality and the Fair Health Information Practices Act of 1997 (H.R. 52). The ACLI is a national trade association with 557 member life insurance companies representing approximately 90 percent of the life insurance in force in the United States. Many of our member companies also sell disability income and long-term care insurance. Life, disability income, and long-term care insurance provide financial security to millions of Americans and help individuals and families achieve their financial goals.

The ACLI is strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their health information and that insurers have an obligation to assure individuals of the confidentiality of that information. As an industry, life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information in a professionally appropriate manner. We are proud of our record as custodians of this information.

The policy position of the ACLI regarding the confidentiality of individually identifiable health information is grounded in our long-standing support of the NAIC Insurance Information and Privacy Protection Model Act (Privacy Model Act). The ACLI believes this model strikes a proper balance between consumers' legitimate expectations of privacy and insurers' information needs. The Privacy Model Act governs insurers' practices in relation to all types of information including individually identifiable health information.

The Privacy Model Act governs the collection of individually identifiable health information and limits redisclosure of that information through, among other things, its requirements relating to notice of information practices and disclosure authorization forms, and its disclosure limitations and conditions. In addition, the Privacy Model Act provides individuals with the right to see and copy personal health information obtained during the underwriting process and to receive a list of those individuals and institutions from which information was obtained and to which information was disclosed, if any. The Privacy Model Act sets forth civil penalties for disclosures or other acts in violation of its requirements.

The ACLI is among the strongest supporters of state regulation of insurance. The ACLI continues to be supportive of the adoption of insurance information and privacy protection

legislation at the state level through the enactment of the Privacy Model Act. However, in recognition of the increased focus at the federal level on possible standards for the confidentiality of medical information, which is likely to result in federal standards in this area, the ACLI will support federal confidentiality standards regarding health information provided, among other things, such standards are substantially similar to those contained in the Privacy Model Act, and the federal legislation contains broad preemption provisions that supersede state privacy laws.

It is essential that life, disability income, and long-term care insurers be able to properly collect, use and redisclose individually identifiable health information as necessary in the ordinary course of business. Otherwise, these insurers will be jeopardized in their ability to continue to underwrite in a fair and financially prudent manner and to evaluate claims pursuant to the terms of their contracts.

Regardless of whether the privacy standards ultimately adopted are intended to directly govern life, disability income, or long-term care insurers' information practices, these insurers will be fundamentally impacted by the standards. This is true because the standards will govern entities, primarily health care providers, from whom life, disability income, and long-term care insurers must collect individually identifiable health information. It is of particular concern because life, disability income, and long-term care insurers' needs and practices in relation to this information are likely to be substantially different from those of other entities, such as health care providers.

A privacy standard which would operate as a prohibition or limitation on third parties' disclosure of individually identifiable health information, including genetic information, to life, disability income, or long-term care insurers, or a standard which would operate as a prohibition

or limitation on such insurers' use of this information, would operate as a prohibition or limitation of medical underwriting by these insurers. This would jeopardize the risk classification process and consequently, insurers' ability to continue to keep life, disability income, and long-term care insurance widely available at affordable prices, as it is now.

Risk classification, based to a large extent on medical underwriting, continues to be the cornerstone of the existing private life, disability income, and long-term care insurance markets. It is a process that involves the separation of applicants into different categories, each category containing insureds with similar risk characteristics and expectations of loss. Risk classification makes it possible for insurers to determine premiums which are fair in relation to the proposed insureds' risk of dying prematurely and premiums which are financially adequate to insure insurers' ability to honor future claims obligations to its policyholders and insureds. Elimination or significant restriction of the risk classification process would necessitate fundamental structural changes to the existing private life, disability income, and long-term care insurance markets. Ultimately, these changes would have to result in some form of socialized risk or public insurance program to satisfy insurance needs now handled privately.

Individually identifiable health information is also essential to life, disability income, and long-term care insurers' ability to evaluate claims. It is often necessary for an insurer to evaluate individually identifiable health information in order to determine appropriate benefits payable under a particular policy. Consequently, a limitation or prohibition on life, disability income and long-term care insurers' information practices could also fundamentally interfere with fulfillment of their contractual obligations to their insureds and policyholders.

In describing the Fair Health Information Practices Act of 1997, the bill's sponsor, Congressman Gary Condit, describes the need to, "strike an appropriate balance that protects each patient's interests while permitting essential uses of data under controlled conditions." We are concerned that, as currently drafted, H.R. 52 may impact insurers selling life, disability income, and long-term care insurance in unintentional ways. We look forward to working with the members and staff of the subcommittee in developing privacy standards which do not inadvertently, but fundamentally, jeopardize the life, disability income and long-term care insurance markets and the financial security of the millions of American consumers insured under these markets.



185

