

## EXTENSIONS OF REMARKS

NATIONAL POLICY CONCERNING  
PRIVACY OF HEALTH CARE  
RECORDS

HON. TED STRICKLAND

OF OHIO

IN THE HOUSE OF REPRESENTATIVES

*Wednesday, May 3, 2006*

Mr. STRICKLAND. Mr. Speaker, on behalf of the National Academies of Practice I would like to submit the National Policy Concerning Privacy of Health Care Records Paper to the CONGRESSIONAL RECORD.

NATIONAL POLICY CONCERNING PRIVACY OF  
HEALTH CARE RECORDS

## SUMMARY

Confidentiality—the understanding that information given in confidence will be held in confidence—has characterized the patient-practitioner relationship for the last 2400 years or more. It has been an essential component of the professional's promise to be a conscientious fiduciary, a promise that has been the cornerstone of patient trust in the health care system.

Privacy—the right of the individual “to be left alone,” a liberty of personal autonomy that the Supreme Court has held to be protected by the 14th Amendment—has been emerging over the last several decades as a salient issue in health care. This emergence is driven by technological changes that have radically altered the ability of confidentiality pledges alone to assure the security of sensitive personal information. Privacy is related to confidentiality but has differing implications that need to be understood.

An effective health care system requires sound public policy that sensitively addresses privacy and confidentiality issues in ways that do not jeopardize the crucial patient-professional relationship and do not impair the practitioner's ability to justify the trust of his/her patients.

Introduction: This paper is a brief description of the issues involved in health care confidentiality and in statutory regulation of patient privacy rights. It suggests the direction that national policy should take in addressing these issues. It reflects the perspective of the National Academies of Practice (NAP), a multidisciplinary body of distinguished health care practitioners that was founded to distill the wisdom of the practice community into functional national health policy.

Confidentiality: Confidentiality is the assurance that information received in confidence will be held in confidence. As part of their ethical commitment, professionals have promised confidentiality of patient information from as long ago as approximately 400 BC, with the introduction of the Hippocratic Oath: “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.” A similar confidentiality promise has been incorporated into almost every ethics code of almost every health care profession since that time. Trust, based in part on assurance of confidentiality, is necessary to achieve open communication and cooperation. Without such trust, professional effectiveness is severely limited or impossible.

The National Consumer Health Privacy Survey of 2005 (California HealthCare Foundation) suggests that this trust is severely stressed in our modern health care system.

Privacy: Privacy, in the words of Justice Louis Brandeis in 1890, is the “right to be left alone.” This right has been held to be supported by the 14th Amendment, and partially supported by the 1st, 4th, and 5th Amendments. In varying degrees, the right has been extended to certain personal records and other information; however, case law and judicial holding about the right to privacy of personal information is still in flux. The November 2, 2005 ruling on No. 04-2550 in the United States Court of Appeals for the Third Circuit, *Citizens for Health v. Leavitt*, suggests that such right may depend more on individual statutes than on constitutional protection.

Privacy was not a traditional consideration in health care, but has become one. The patient does not want to be “left alone” in the treatment relationship, but does want his or her health information to be held in confidence. Traditionally, when only the professional had access to the record, usually a hand-written notation in his or her private file, privacy of the record itself was automatic so long as confidentiality was maintained. Today, good health care requires that the professional's findings be entered into a permanent health care record that is available to multiple other parties. When that happens, the professional loses control of the information, and only protection of the record itself can assure professional confidentiality. That protection is directly dependent on privacy policies or laws that fall under statutory rather than professional control.

Adjudication of privacy rights under law, especially the extension of those rights to health record information, did not have its origin in health care concerns. Here, people writing privacy policy tend to be unfamiliar with the tradition of health care and confidentiality, just as health care providers, steeped in the tradition of confidentiality as an ethical commitment, tend to be uninformed about the nuances of privacy law. The hazard is great that health care practitioners, with the wisdom of the ages behind them in building necessary patient trust, will be ignored in the development of privacy law and that those who develop privacy policy will be insensitive to the critical nature of the patient-practitioner relationship. At risk is the functionality of health care delivery, one of the most humanely important and economically significant enterprises in the country.

Cultural Shift from Confidentiality as Sole Protector of Privacy: The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and other groups require accredited facilities to have in place patient's rights regulations that protect sensitive health information. As noted, the safety of such records can no longer depend on confidentiality agreements alone. Privacy of the health care record itself has to be assured. Extensive national policy positions have recently been established to address the privacy issue. The most notable is the Health Insurance Portability and Accountability Act (HIPAA), which laudably adds many necessary patient protections. Health care professionals nevertheless find HIP AA to be

both ineffective and burdensome in certain key respects. Future refinements are clearly needed. Understanding the shift from exclusive reliance on confidentiality to the need for privacy laws can point toward effective solutions. Four trends warrant highlighting.

Numerous health care professionals, third party payers, employers, and support personnel are routinely involved in today's health care system. The health care record has become the medium of communication among these involved groups. The health care professional can neither functionally withhold sensitive information from the record nor control the use of that information by others. The old promise of confidentiality is therefore no longer adequate protection of the sensitive information.

Technology has greatly increased the amount of sensitive information that directly enters the record, information that is not directly under the practitioner's control. These data include X-rays, blood chemistries, and numerous other laboratory or technologist-based findings. At the same time, the need for these laboratory personnel and technologists, as well as insurers, consultants, and others, to have access to health care information increases. All of these developments magnify the importance of controlling the health care record itself and its use by everyone with access to it.

The growing complexity of the health care system places increasing demands on the health care record. In response, the information age is replacing traditional multiple written records with a single electronically encoded one that can be accessed by almost any properly prepared person almost anywhere on earth. This shift to an agglomerated record in electronic format greatly magnifies the utility of the record as an aide to effective health care. At the same time, it creates a nightmare for control of privacy of the information it contains. Not only are confidentiality pledges inadequate but so also are privacy laws that cannot prevent hacking and other forms of electronic information theft.

The primary ingredient of effective health care over the last 2400 years or so has been the commitment of health care professionals to be conscientious fiduciaries. That continues to be the primary ingredient, but one that is being increasingly obfuscated by the shift from guild control to legal control of health care practice. As already noted, laws are necessary to implement privacy rights. Similarly, legally enforced licensing laws have replaced guild control of code of conduct issues, and the growing complexity of the health care system has interfaced health care with the legal system as never before. The result has been a tendency to raise both public and regulatory expectation that legal mandate can guarantee professional integrity. In fact, laws can supplement but cannot guarantee or replace professional integrity, which is as critical today for effective health care as it ever was. How far this muddying of the critical importance of the professional relationship will go remains to be seen. In the mean time, it creates a pressure for the professional to shift away from “caring” practice to “safe” practice and for the patient to shift away from a “trusting” attitude to a “litigious” attitude. Both of these trends are often at the expense of effectiveness of treatment and economy of service delivery. The shift toward legal regulation is

• This “bullet” symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.

Matter set in this typeface indicates words inserted or appended, rather than spoken, by a Member of the House on the floor.

inevitable, so the sensitivity with which policies and laws are drafted is absolutely critical for the future health of the nation.

The foregoing are dramatic changes in long-accepted traditions. Privacy of the health care record, legally regulated, is the visible "new kid on the block." Unlike professional confidentiality, it has little "wisdom of history" behind it. Not surprisingly, there is a tendency to address privacy by tactics that might work for confidentiality but do not work for privacy, by placing heavy penalties on professional breaches. This is ineffective when little attention is given to the leaky-sieve aspects of the health care record system itself. In fact, it can be severely counter-productive if it poisons the traditional trusting relationship between patient and professional. The urgent need is for highly sensitive and highly enlightened health care policy that preserves the wisdom of the past.

**Tentative Answers to Complex Questions:** Five questions arise in the context of the new privacy era in health care.

1. How extensive should the health care record be? The health care record will, and should, become increasingly complex and extensive. Information technology allows the retention and utilization of vast quantities of information. The future health care record will almost certainly be in electronic form. With electronic data manipulation techniques, even an extensive record can be efficiently sorted to allow quick decisions about immunizations, allergies, past responses to specific treatment approaches, drug interaction risks, excessive or inappropriate drug use, and similar questions of care. Aggregated data across a given problem or disease spectrum could identify both promising and ineffective treatment approaches. The potential gain from having such records is impressive indeed, and the technology for collecting, preserving, and utilizing them is already largely in place.

2. Who should have access to what information? Portions of the health care record should be accessible by every health care practitioner with whom each client will potentially interact. Other portions should be accessible by insurers, managed care officials, and similar non-health-care personnel who have a direct and necessary "need to know." Portions should be available for malpractice monitoring and similar purposes. Portions should be available to research programs, perhaps stripped of data identifying the individual source. The number of people who should have legitimate access, in the interest of improving the health of both our individual citizens and the nation itself, will inevitably grow.

3. How can access be made easy on a "need to know" basis? In this electronic age, partitioning the record for limited access is technologically easy. For example, a school nurse needing to certify an immunization record neither needs nor wants to sort through the entire record. An electronic summary of immunizations can be programmed into the record and be made immediately available to a coded request by a "school health worker." Similarly, current health status and current proposed or completed treatments can be electronically isolated for benefit of reimbursement or managed care assessments without exposure of the entire chart. The mental health record can be sequestered, with access limited to those with legitimate interest in that area. In general easy electronic access to appropriate data can be designed into the system, provided inappropriate policies do not frustrate legitimate access in the name of security.

4. How can inappropriate access be prevented? Any effective solution requires that

the electronic record itself be designed from the beginning to incorporate essentially fool-proof security features. In the past, "loose lips" were the primary problem, people with legitimate information intentionally or unintentionally leaking that information. Control of people was the primary solution. Within the health care professions, lapse of confidentiality has long been addressed by guild ethics and by licensing laws that regulate the actions of the professionals. Outside of the health care professions, especially in the economic sector, abuse of confidentiality still needs to be addressed more effectively.

Although important, loose lips are not the primary problem. They usually endanger only one person at a time, rather than thousands whose data may be accessible in the electronic record. Limiting access to the electronic record to those with a legitimate need to know is the most significant key to guaranteeing privacy. Electronic data can be hacked, copied, transported, collected, sold, and otherwise manipulated in ways that are difficult to detect by people who are hard to identify. Passwords and other access codes, encryption, and the like may be essential, but they are not enough. The Internet, the primary platform for current electronic data portability, has not yet achieved the levels of security that are necessary.

A workable system might involve a completely separate health information network operating out of a centralized data bank and accessible only through authorized terminals. Security might involve requiring bio-electronic screening for palm prints, iris patterns, voice prints, or the like prior to system access. Electronic "footprints," or audit trails, could preserve a record of all data accessed and for what purposes. An alarm system could alert a central information-monitoring group when an unauthorized access was attempted or when an unusual pattern of access was detected. Such steps would make unwarranted penetration of the system rare, access to the system by authorized persons easy, and apprehension of violators probable.

5. Who should control the privacy information? Privacy rights should guarantee that health care information is held confidential within the health care system, except as the patient explicitly opts out of the privacy agreement. It is the patient's knowledge that his or her own sensitive information will be used only for health care purposes that assures the trust necessary for effective cooperation. Circulation of the information within the legitimate health care system is necessary and functional, but circulation outside of that system, without explicit and uncoerced patient consent, should be taboo. Public knowledge of personal health problems can be severely damaging. One only has to recall Eagleton's vice-presidential nomination.

A few legally mandated requirements, such as the duty to protect or the duty to alert authorities of abuse of helpless patients, currently require exceptions to confidentiality. Perhaps other exceptions are warranted, but professional experience suggests that they should be rare and very carefully crafted. We suggest that they should be limited to those circumstances that pose an explicit future threat to others or an abuse against which a patient is not capable of protecting himself/herself.

While a patient may voluntarily choose to waive some privacy rights, perhaps in exchange for convenience or other benefits, waivers that are determined by law as part of health care policy, as in certain sections of HIPAA, are often more disclosure notices than they are matters of voluntary consent. Without true voluntary consent, there is no choice and no trust. These complexities re-

fect the early growing pains of privacy law and can have serious unintended consequences.

It is in these areas of developing health care policy and related privacy law that health care practitioners can make some of their most important policy contributions. The danger is that others who determine such policies may either fail to understand or simply disregard the practitioner perspective, at great harm to the nation's health.

**Conclusions:** Practitioner work is anchored on two premises that have stood the test of time: patient trust, which is necessary for essential communication, and the guarantee of confidentiality of information, which requires that the health care record be used exclusively for health care purposes. The National Academies of Practice recommends that information in the health care record should be exclusively available for health care purposes and that the record should be protected from access for any other use.

Maintaining privacy with an ever expanding and easily accessible electronic health care record, in an ever more complex health care delivery system, requires new approaches. These approaches must be integrated into the record keeping and service delivery systems themselves, through technological safeguards. Health care practitioners cannot control the privacy of the health record and do not control privacy policy, but our long experience with confidentiality issues and our pragmatic wisdom concerning the treatment process offer understanding that should be an essential part of policy development.

Some present trends in national privacy policy are threatening the integrity of the practitioner/patient relationship. A sensitive and sophisticated privacy policy for health care records that does not jeopardize the necessary trust of the patient is critical to assure the effectiveness of health service delivery. Health care professionals that represent the wisdom of the multidisciplinary practitioner community are an indispensable resource for such policy development. Failure to incorporate them, visibly and functionally, into the policy making process risks jeopardizing the millennia-long practitioner tradition of establishing consumer trust on which the effectiveness of health care depends.

---

## THE POLICE UNITY TOUR

**HON. RODNEY P. FRELINGHUYSEN**

OF NEW JERSEY

IN THE HOUSE OF REPRESENTATIVES

*Wednesday, May 3, 2006*

Mr. FRELINGHUYSEN. Mr. Speaker, I rise today to honor the Police Unity Tour. On May 9th, the Police Unity Tour will kick-off their 10th anniversary bicycle tour to our Nation's capitol.

For the past nine years, police officers have mounted their bicycles and cycled from New Jersey to Washington, DC, in memory of the men and women of the police force, who have sacrificed their lives while protecting our communities from harm. This year, the ride will begin on May 9 and end on May 13. The officers will depart from the Florham Park Police Headquarters, in Florham Park, NJ and will arrive at the National Law Enforcement Officer's Memorial in Washington, DC, culminating their journey with a candlelight vigil.