

Department of Health and Human Services

§ 164.402

APPENDIX A TO SUBPART C OF PART 164—SECURITY STANDARDS: MATRIX

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
Security Management Process .....	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility .....	164.308(a)(2)	Authorization and/or Supervision (A)
Workforce Security .....	164.308(a)(3)	Workforce Clearance Procedure Termination Procedures (A)
Information Access Management .....	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training .....	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures .....	164.308(a)(6)	Response and Reporting (R)
Contingency Plan .....	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation .....	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)
<b>Physical Safeguards</b>		
Facility Access Controls .....	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use .....	164.310(b)	(R)
Workstation Security .....	164.310(c)	(R)
Device and Media Controls .....	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
<b>Technical Safeguards</b> (see § 164.312)		
Access Control .....	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls .....	164.312(b)	(R)
Integrity .....	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication .....	164.312(d)	(R)
Transmission Security .....	164.312(e)(1)	Integrity Controls (A) Encryption (A)

**Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

**§ 164.400 Applicability.**

The requirements of this subpart shall apply with respect to breaches of

protected health information occurring on or after September 23, 2009.

**§ 164.402 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.