

the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications* (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

§164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with §164.306:

(a) *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation.* (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

§164.318 Compliance dates for the initial implementation of the security standards.

(a) *Health plan.* (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

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

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R)

§ 164.400

45 CFR Subtitle A (10–1–10 Edition)

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

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.

(1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or