

# HIPAA Privacy

*An innovative approach to self-implementation*

# WorkGroups®

## Security Series

### **TITLE 45--PUBLIC WELFARE AND HUMAN SERVICES**

### **Subpart C--Security Standards for the Protection of Electronic Protected Health Information**

### **Teleconference Supplement**

February, 2004

© Gregory D. Frost 2003, 2004



## TITLE 45--PUBLIC WELFARE AND HUMAN SERVICES

### Subpart C--Security Standards for the Protection of Electronic Protected Health Information

#### **Sec 164.302. Applicability**

#### **Sec 164.304. Definitions**

#### **Sec 164.306. Security standards: General rules**

- (a) General requirements
- (b) Flexibility of approach
- (c) Standards
- (d) Implementation specifications
- (e) Maintenance

#### **Sec 164.308. Administrative safeguards**

- (a) (1) (i) Standard: Security management process
- (ii) Implementation specifications:
  - (A) Risk analysis (Required)
  - (B) Risk management (Required)
  - (C) Sanction policy (Required)
  - (D) Information system activity review (Required)
- (2) Standard: Assigned security responsibility
- (3) (i) Standard: Workforce security
- (ii) Implementation specifications:
  - (A) Authorization and/or supervision (Addressable)
  - (B) Workforce clearance procedure (Addressable)
  - (C) Termination procedures (Addressable)
- (4) (i) Standard: Information access management
- (ii) Implementation specifications:
  - (A) Isolating health care clearinghouse functions (Required)
  - (B) Access authorization (Addressable)
  - (C) Access establishment and modification (Addressable)
- (5) (i) Standard: Security awareness and training
- (ii) Implementation specifications
  - (A) Security reminders (Addressable)
  - (B) Protection from malicious software (Addressable)
  - (C) Log-in monitoring (Addressable)
  - (D) Password management (Addressable)
- (6) (i) Standard: Security incident procedures
- (ii) Implementation specification: Response and Reporting (Required)
- (7) (i) Standard: Contingency plan
- (ii) Implementation specifications:
  - (A) Data backup plan (Required)
  - (B) Disaster recovery plan (Required)
  - (C) Emergency mode operation plan (Required)
  - (D) Testing and revision procedures (Addressable)
  - (E) Applications and data criticality analysis (Addressable)
- (8) Standard: Evaluation
- (b) (1) Standard: Business associate contracts and other arrangements

**Sec 164.310. Physical safeguards**

- (a) (1) Standard: Facility access controls.
- (2) Implementation specifications:
  - (i) Contingency operations (Addressable).
  - (ii) Facility security plan (Addressable).
  - (iii) Access control and validation procedures (Addressable).
  - (iv) Maintenance records (Addressable).
- (b) Standard: Workstation use.
- (c) Standard: Workstation security.
- (d) (1) Standard: Device and media controls.
- (2) Implementation specifications:
  - (i) Disposal (Required).
  - (ii) Media re-use (Required).
  - (iii) Accountability (Addressable).
  - (iv) Data backup and storage (Addressable).

**Sec 164.312. Technical safeguards**

- (a) (1) Standard: Access control.
- (2) Implementation specifications:
  - (i) Unique user identification (Required).
  - (ii) Emergency access procedure (Required).
  - (iii) Automatic logoff (Addressable).
  - (iv) Encryption and decryption (Addressable).
- (b) Standard: Audit controls.
- (c) (1) Standard: Integrity.
- (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).
- (d) Standard: Person or entity authentication.
- (e) (1) Standard: Transmission security.
- (2) Implementation specifications:
  - (i) Integrity controls (Addressable).
  - (ii) Encryption (Addressable).

**Sec 164.314. Organizational requirements**

- (a) (1) Standard: Business associate contracts or other arrangements
- (2) Implementation specifications (Required)
  - (i) Business associate contracts
  - (ii) Other arrangements
- (b) (1) Standard: Requirements for group health plans
- (2) Implementation specifications (Required)

**Sec 164.316. Policies and procedures and documentation requirements**

- (a) Standard: Policies and procedures.
- (b) (1) Standard: Documentation.
- (2) Implementation specifications:
  - (i) Time limit (Required).
  - (ii) Availability (Required).
  - (iii) Updates (Required).

**Sec 164.318. Compliance dates for the initial implementation of the security standards**

- (a) Health plan.
- (b) Health care clearinghouse.
- (c) Health care provider.

## Subpart C--Security Standards for the Protection of Electronic Protected Health Information<sup>1</sup>

**§ 164.302 Applicability.** A covered entity must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information.

**Sec. 164.304 Definitions.** As used in this subpart, the following terms have the following meanings:

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part.)

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

*Authentication* means the corroboration that a person is the one claimed.

*Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Security* or *Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

---

<sup>1</sup> Authority: 42 U.S.C. 1320d-2 and 1320d-4.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

### **Sec. 164.306 Security standards: General rules.**

(a) *General requirements.* Covered entities must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

(b) *Flexibility of approach.*

- (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
- (2) In deciding which security measures to use, a covered entity must take into account the following factors:
  - (i) The size, complexity, and capabilities of the covered entity.
  - (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
  - (iii) The costs of security measures.
  - (iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity must comply with the standards as provided in this section and in Sec. 164.308, Sec. 164.310, Sec. 164.312, Sec. 164.314, and Sec. 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

- (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in Sec. 164.308, Sec. 164.310, Sec. 164.312, Sec. 164.314, or Sec. 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

(1) [sic] When a standard adopted in Sec. 164.308, Sec. 164.310, Sec. 164.312, Sec. 164.314, or Sec. 164.316 includes addressable implementation specifications, a covered entity must--

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the entity--

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate--

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under Sec. 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at Sec. 164.316.

### **Sec. 164.308 Administrative safeguards.**

(a) A covered entity must, in accordance with Sec. 164.306:

(1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required).<sup>2</sup> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities<sup>3</sup> to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.<sup>4</sup>

---

<sup>2</sup> “An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities.” Preamble to final Security Standards, 68 FR 8334, 8346.

<sup>3</sup> Including a “threat assessment”. See Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>4</sup> “A thorough and accurate risk analysis would consider ‘all relevant losses’ that would be expected if the security measures were not in place. ‘Relevant losses’ would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures.” Preamble to final Security Standards, 68 FR 8334, 8347.

See, also, §306(e),

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level<sup>5</sup> to comply with Sec. 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions<sup>6</sup> against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) Information system activity review<sup>7</sup> (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) Standard: Assigned security responsibility. Identify the<sup>8</sup> security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.<sup>9</sup>

(3) (i) Standard: Workforce security.<sup>10</sup> Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) Implementation specifications:

(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) Workforce clearance procedure (Addressable).<sup>11</sup> Implement procedures<sup>12</sup> to determine that the access<sup>13</sup> of a workforce member<sup>14</sup> to electronic protected health information is appropriate.

---

<sup>5</sup> “If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so.” Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>6</sup> “The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.” Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>7</sup> “Our intent for this requirement was to promote the periodic review of an entity’s internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity’s security environment.” Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>8</sup> “[F]inal rule specifies that final security responsibility must rest with one individual to ensure accountability within each covered entity. More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity’s electronic protected health information.” Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>9</sup> “The same person could fill the role for both security and privacy.” Preamble to final Security Standards, 68 FR 8334, 8347.

<sup>10</sup> “Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below).” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>11</sup> “For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse.” Preamble to final Security Standards, 68 FR 8334, 8348.

<sup>12</sup> “The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place.” Preamble to final Security Standards, 68 FR 8334, 8348.

<sup>13</sup> “We note that a covered entity should consider in this regard the applicable requirements of the Privacy Rule”. Preamble to final Security Standards, 68 FR 8334, 8348.

<sup>14</sup> “[F]or example, operations and maintenance personnel”. Preamble to final Security Standards, 68 FR 8334, 8348.

(C) Termination procedures (Addressable)<sup>15</sup>. Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.<sup>16</sup>

(4) (i) Standard: Information access management.<sup>17</sup> Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable).<sup>18</sup> Implement policies and procedures for granting access to electronic protected health information,<sup>19</sup> for example, through access to a workstation, transaction, program, process, or other mechanism.<sup>20</sup>

(C) Access establishment and modification (Addressable).<sup>21</sup> Implement policies and procedures that, based upon the entity's access authorization policies, establish, document<sup>22</sup>, review, and modify a user's right of access to a workstation, transaction, program, or process.

---

<sup>15</sup> “This is addressable because in certain circumstances, for example, a solo physician practice whose staff consists only of the physician’s spouse, formal procedures may not be necessary. ... [C]onsideration of termination procedures remains relevant for any covered entity with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain.” Preamble to final Security Standards, 68 FR 8334, 8348 - 9.

<sup>16</sup> “The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving keys a termination occurs.” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>17</sup> “... both the establishment of access control policies and their implementation.” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>18</sup> “These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications.” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>19</sup> “We cannot, however, specifically identify participating parties and access privileges relative to data elements within this regulation. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with ... minimum necessary requirements ....” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>20</sup> “The process of managing access involves allowing and restricting access to those individuals that have been authorized to access the data. The intent of the proposed authorization control implementation feature [45 CFR 164.308(c)(1)(iii) at 63 FR 43242, 43268] is now incorporated in the access authorization implementation specification under the information access management standard in § 164.308(a)(4). Under the information access management standard, a covered entity must implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access. These policies and procedures will enable entities to follow the Privacy Rule minimum necessary requirements, which provide when persons should have access to information.” 68 FR 8334, 8349.

<sup>21</sup> “These specifications may not be applicable to all entities based on their size and degree of automation. A fully automated covered entity spanning multiple locations and involving hundreds of employees may determine it has a need to adopt a formal policy for access authorization, while a small provider may decide that a desktop standard operating procedure will meet the specifications.” Preamble to final Security Standards, 68 FR 8334, 8349.

<sup>22</sup> “[D]ocumentation should be an official organizational statement as opposed to word-of-mouth or cryptic notes scratched on a notepad.” Preamble to final Security Standards, 68 FR 8334, 8349.

(5) (i) Standard: Security awareness and training.<sup>23</sup> Implement a security awareness and training program for all members of its workforce<sup>24</sup> (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6) (i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity<sup>25</sup>; and document security incidents and their outcomes.

(7) (i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures<sup>26</sup> for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

---

<sup>23</sup> “Security awareness training is a critical activity, regardless of an organization’s size. This feature would typically become part of an entity’s overall training program (which would include privacy and other information technology items as well). For example, the Government Information Systems Reform ACT (GISRA) of 2000 requires security awareness training as part of Federal agencies’ information security programs, including Federal covered entities, such as the Medicare program. In addition, National Institute of Standards and Technology (NIST) SP 800–16, *Information Technology Security Training Requirements, A role and performance base model, April 1998*, provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities. ... [T]he amount and type of training needed will be dependent upon an entity’s configuration and security risks. ... This requirement does not mean lengthy training is appropriate in every instance; there are alternative methods to inform individuals of security responsibilities (for example, provisions of pamphlets or copies of security policies, and procedures). ... Amount and timing of training should be determined by each covered entity; training should be an ongoing, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. Preamble to final Security Standards, 68 FR 8334, 8350.

<sup>24</sup> “Covered entities are not required to provide training to business associates or anyone else that is not a member of their workforce.” Preamble to final Security Standards, 68 FR 8334, 8350.

<sup>25</sup> See, also, mitigation requirement in 45 CFR §164.530(f).

<sup>26</sup> “The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it.” Preamble to final Security Standards, 68 FR 8334, 8351.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.<sup>27</sup>

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform<sup>28</sup> a periodic<sup>29</sup> technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

(b) (1) Standard: Business associate contracts and other arrangements.<sup>30</sup> A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate will appropriately safeguard the information.

(2) This standard does not apply with respect to--

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.<sup>31</sup>

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of Sec. 164.314(b) and Sec. 164.504(f) apply and are met;<sup>32</sup> or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at Sec. 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of Sec. 164.502(e)(1)(ii)(C) are met.<sup>33</sup>

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and Sec. 164.314(a).<sup>34</sup>

<sup>27</sup> “[D]uring and immediately after a crisis situation.” Preamble to final Security Standards, 68 FR 8334, 8351.

<sup>28</sup> “Evaluation by an external entity is a business decision to be left to each covered entity. Evaluation is required under § 164.308(a)(8), but a covered entity may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.” Preamble to final Security Standards, 68 FR 8334, 8351.

<sup>29</sup> “Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation, for example, new technology adopted or responses to newly recognized risks to the security of their information.” Preamble to final Security Standards, 68 FR 8334, 8351.

<sup>30</sup> Compare to 45 CFR §164.502(e)(1)(i).

<sup>31</sup> Compare to 45 CFR §164.502(e)(1)(ii)(A).

<sup>32</sup> Compare to 45 CFR §164.502(e)(1)(ii)(B).

<sup>33</sup> Compare to 45 CFR §164.502(e)(1)(ii)(C).

<sup>34</sup> Compare to 45 CFR §164.502(e)(1)(iii).

(4) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a).<sup>35</sup>

**Sec. 164.310 Physical safeguards.**<sup>36</sup> A covered entity must, in accordance with Sec. 164.306:

(a) (1) Standard: Facility<sup>37</sup> access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations<sup>38</sup> (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures<sup>39</sup> to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) Standard: Workstation<sup>40</sup> use. Implement policies and procedures that specify the proper functions to be performed<sup>41</sup>, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

<sup>35</sup> Compare to 45 CFR §164.502(e)(2).

<sup>36</sup> “Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” 45 CFR 164.304.

“This final rule does not preclude the use of electronic security systems in lieu of, or in combination with, physical security systems to meet a “Physical safeguard” standard.” Preamble to final rule, 68 FR 8353.

<sup>37</sup> Facility means the physical premises and the interior and exterior of a building(s).” 45 CFR 164.304.

<sup>38</sup> See, also, 45 CFR 164,308(a)(7) “Contingency Plans”.

<sup>39</sup> “[T]he covered entity retains responsibility for considering facility security even where it shares space within a building with other organizations. Facility security measures taken by a third party must be considered and documented in the covered entity’s facility security plan, when appropriate.” Preamble to final rule, 68 FR 8353.

<sup>40</sup> “Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.” 45 CFR 164.304.

<sup>41</sup> “[F]or example, logging off before leaving a workstation unattended ....” Preamble to final rule, 68 FR 8354.

- (c) Standard: Workstation<sup>42</sup> security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
- (d) (1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media<sup>43</sup> that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
- (2) Implementation specifications:
- (i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
  - (ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
  - (iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
  - (iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

**Sec. 164.312 Technical safeguards.**<sup>44</sup> A covered entity must, in accordance with Sec. 164.306:

- (a) (1) Standard: Access control.<sup>45</sup> Implement technical policies and procedures<sup>46</sup> for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).
- (2) Implementation specifications:
- (i) Unique user identification<sup>47</sup> (Required). Assign a unique name and/or number for identifying and tracking user identity.

---

<sup>42</sup> “*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.” 45 CFR 164.304.

<sup>43</sup> “[F]or example, diskettes and tapes ....” Preamble to final rule, 68 FR 8354.

<sup>44</sup> Other requirements related to Technical Safeguards include (1) information access management, §308(a)(4); (2) protection from malicious software, §308(a)(5)(ii)(B); log-in monitoring §308(a)(5)(ii)(C); password management §308(a)(5)(ii)(D); security incident identification §308(a)(6)(ii); data back-up §308(a)(7)(ii)(A); and workstation security §310(c).

For original version, see proposed rule 45 CFR 164.308(c) and (d) at 63 FR 43242, 43268.

<sup>45</sup> Types of access control listed in the proposed rule “include, among others, mandatory access control, discretionary access control, time-of day, classification, and subject-object separation.” 63 FR 43242, 43254

<sup>46</sup> The proposed security rule at 45 CFR 164.308(c)(1)(i)(B) required the use of at least one of the following: (1) Context -based access (an access control procedure based on the context of a transaction (as opposed to being based on attributes of the initiator or target)); (2) Role-based access; (3) User-based access.” In response to comments, HHS noted: “We agree ... that other types of access controls should be allowed. There was no intent to limit the implementation features to the named technologies and this final rule has been reworded to make it clear that use of any appropriate access control mechanism is allowed.” 68 FR 8334, 8355

(ii) Emergency access procedure<sup>48</sup> (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff<sup>49</sup> (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption<sup>50</sup> (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls.<sup>51</sup> Implement hardware, software, and/or procedural mechanisms that record and examine activity<sup>52</sup> in information systems that contain or use electronic protected health information.

(c) (1) Standard: Integrity<sup>53</sup>. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.<sup>54</sup>

---

<sup>47</sup> “Automatic logoff” and “Unique user identification” were formerly implementation features under the proposed “Entity authentication” (see § 164.312(d)).

<sup>48</sup> “Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.” 68 FR 8334, 8355.

Compare to contingency operations in physical safeguards requirements - 45 CFR § 164.310 (a)(2)(i).

<sup>49</sup> “Automatic logoff” and “Unique user identification” were formerly implementation features under the proposed “Entity authentication” (see § 164.312(d)).

“The proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification, [based ... on the particular configuration in use and a risk assessment/analysis] and also permits the use of an equivalent measure.” 68 FR 8334, 8355

<sup>50</sup> “The use of file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, which is a form of control. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity’s risk analysis. Therefore, encryption has been adopted as an addressable implementation specification in this final rule.” 68 FR 8334, 8355

<sup>51</sup> Audit controls “would be important so that the organization can identify suspect data access activities, assess its security program, and respond to potential weaknesses.” 63 FR 43242, 43254

“Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. For example, see NIST Special Publication 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* and NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*.... We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be.” 68 FR 8334, 8355

<sup>52</sup> “There has been a tendency to assume that this Privacy Rule requirement would be satisfied via some sort of process involving audit trails. We caution against assuming that the Security Rule’s requirement for an audit capability will satisfy the Privacy Rule’s requirement regarding accounting for disclosures of protected health information. The two rules cover overlapping, but not identical information. Further, audit trails are typically used to record uses within an electronic information system, while the Privacy Rule requirement for accounting applies to certain disclosures outside of the covered entity (for example, to public health authorities).” 68 FR 8334, 8355

<sup>53</sup> Titled data authentication in the proposed rule. Also includes the message authentication implementation specification contained in the proposed rule. (45 CFR 164.308(d)(1)(i)(B), 63 FR 43242, 43268).

<sup>54</sup> “Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanisms that are ubiquitous in hardware and operating systems today. The risk analysis process will address what data must be authenticated and should provide

(d) Standard: Person or entity authentication. Implement procedures<sup>55</sup> to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) (1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted<sup>56</sup> over an electronic communications network.<sup>57</sup>

(2) Implementation specifications:

(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.<sup>58</sup>

---

answers appropriate to the different situations faced by the various health care entities implementing this regulation. Further, we believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task.” 68 FR 8334, 8356. The proposed rule also lists “a message authentication code” as an example of a data authentication tool. 63 FR 43242, 43254.

<sup>55</sup> “‘Digital signatures’ and ‘soft tokens’ may be used, as well as many other mechanisms, to implement this standard.” 68 FR 8334, 8356. The proposed rule also listed “Automatic log off; Unique user identification; a biometric identification system; a password system; a personal identification number (PIN) ; telephone callback; a token system which uses a physical device for user identification.” 63 FR 43242, 43254.

<sup>56</sup> Covered entities are not responsible for “the unsolicited electronic receipt of health information in an unsecured manner, for example, when the information was submitted by a patient via e-mail over the Internet”, but are required to protect the information once received. 68 FR 8334, 8357.

<sup>57</sup> “When electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk.” 68 FR 8334, 8356.

“This final rule has been revised to reflect deletion of the following implementation features: (1) The alarm capability; (2) audit trail; (3) entity authentication; and (4) event reporting. These features were associated with a proposed requirement for ‘Communications/network controls’ and have been deleted since they are normally incorporated by telecommunications providers as part of network management and control functions that are included with the provision of network services. A health care entity would not expect to be responsible for these technical telecommunications features.” 68 FR 8334, 8357.

<sup>58</sup> “Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.” 68 FR 8334, 8357. The proposed rule noted that “the utilization of less open systems/networks such as those provided by a value-added network (VAN) or private-wire arrangement provides sufficient access controls to allow encryption to be an optional feature.” FR 43242, 43255. Similarly, the final rule stated that “encryption should not be a mandatory requirement for transmission over dial-up lines.” 68 FR 8334, 8357.

**Sec. 164.314 Organizational requirements.**

(a) (1) Standard: Business associate contracts or other arrangements.<sup>59</sup>

(i) The contract or other arrangement between the covered entity and its business associate required by Sec. 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii)<sup>60</sup> A covered entity is not in compliance with the standards in Sec. 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful--

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) Implementation specifications (Required).

(i) Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will--

(A)<sup>61</sup> 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 covered entity as required by this subpart;

(B)<sup>62</sup> Ensure that any agent, including a subcontractor<sup>63</sup>, to whom it provides such information agrees to implement reasonable and appropriate safeguards<sup>64</sup> to protect it;

(C)<sup>65</sup> Report to the covered entity any security incident of which it becomes aware;

(D)<sup>66</sup> Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

<sup>59</sup> Compare to 45 CFR §164.504(e).

<sup>60</sup> Functionally identical to 45 CFR §165.504(e)(1)(ii).

<sup>61</sup> This requirement is more detailed than its counterpart at 45 CFR §164.504(e)(2)(ii)(B).

<sup>62</sup> Compare to 45 CFR §164.504(e)(2)(ii)(D).

<sup>63</sup> “In contrast, when another entity is not acting as a business associate for the covered entity, but rather is acting in the capacity of some other sort of trading partner, we do not require the covered entity to require the other entity to adopt particular security measures, as previously proposed.” Preamble to final Security Standards, 68 FR 8334, 8360.

“This final rule does not, however, prohibit a covered entity from employing more stringent security measures or from requiring a business associate to employ more stringent security measures.” *Ibid.*

<sup>64</sup> “The level of security afforded particular electronic protected health information should not decrease just because the covered entity has made the business decision to entrust a business associate with using or disclosing that information in connection with the performance of certain functions instead of doing those functions itself.” Preamble to final Security Standards, 68 FR 8334, 8360.

<sup>65</sup> Compare to 45 CFR §164.504(e)(2)(ii)(C).

<sup>66</sup> Identical to 45 CFR §164.504(e)(2)(iii).

(ii) Other arrangements<sup>67</sup>.

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if--

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in Sec. 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(b) (1) Standard: Requirements for group health plans.<sup>68</sup> Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to Sec. 164.504(f)(1)(ii) or (iii), or as authorized under Sec. 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by 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 Sec. 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.

<sup>67</sup> Functionally equivalent to 45 CFR §164.504(e)(3).

<sup>68</sup> Compare to 45 CFR §164.504(f).

**Sec. 164.316 Policies and procedures and documentation requirements.** A covered entity must, in accordance with Sec.164.306:

(a) Standard: Policies and procedures.<sup>69</sup> 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 Sec. 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.<sup>70</sup>

(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.

**Sec. 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.

---

<sup>69</sup> Compare to 45 CFR §164.530(i).

<sup>70</sup> Compare to 45 CFR §164.530(j).