§ § 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, delete, transmit, or communicate data/information or otherwise use any component of an information system resource. (This definition applies to "access" as used in this subpart, not as used in subpartssubpart D or E of this part.)

Administrative safeguards are administrative actions, and related policies and procedures, to manage the selection, development, implementation, and maintenance (including updating and modifying) of security measures to protect electronic protected health information, and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication means the corroboration that a person or technology asset is the one claimedthey are claiming to be.

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

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

Deploy means to configure technology for use and implement such technology.

Electronic information system means interconnected set of electronic information resources under the same direct management control that shares common functionality. An electronic information system generally includes technology assets, such as hardware, software, electronic media, information, and data.

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).

Implement means to put into effect and be in use, operational, and function as expected throughout the covered entity or business associate.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. AAn information system normallygenerally 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.

Malicious software means software or firmware intended to perform an unauthorized action or activity that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of electronic protected health information. Examples include but are not limited to viruses, worms, Trojan horses, spyware, and some forms of adware.

Multi-factor authentication means authentication of the user's identity through verification of at least two of the following three categories:

(1) Information known by the user, including but not limited to a password or personal identification number (PIN).

(2) Item possessed by the user, including but not limited to a token or a smart identification card.

(3) Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.

Password means confidential authentication information composed of a string of characters~~.~~, such as letters, numbers, spaces, and other symbols.

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

Relevant electronic information system means an electronic information system that creates, receives, maintains, or transmits electronic protected health information or that otherwise affects the confidentiality, integrity, or availability of electronic protected health information.

Risk means the extent to which the confidentiality, integrity, or availability of electronic protected health information is threatened by a potential circumstance or event.

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

Security incident means any of the following:

(1) The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information ~~or interference with system operations~~ in an information system.

(2) The attempted or successful unauthorized interference with system operations in an information system.

Technical controls means the technical mechanisms contained in the hardware, software, or firmware components of an electronic information system that are primarily implemented and executed by the electronic information system to protect the information system and data therein.

Technical safeguards means the technology ~~and the policy~~, technical controls, and related policies and procedures ~~for its~~governing the use ~~that protect~~ of the technology that protects and controls access to electronic protected health information ~~and control access to it.~~.

Technology asset means the components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data.

Threat means any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of electronic protected health information.

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

Vulnerability means a flaw or weakness in an information system, information system security procedures, design, implementation, or technical controls that could be intentionally exploited or accidentally triggered by a threat.

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. Workstation includes but is not limited to the following types of devices: a server, desktop computer, laptop computer, virtual device, and mobile device such as a smart phone or tablet.

164.306 Security standards: General rules.

(a) *General requirements.* ~~Covered entities~~ Each covered entity and business ~~associates~~associate must do the following~~:~~ with respect to all electronic protected health information it creates, receives, maintains, or transmits:

(1) Ensure the confidentiality, integrity, and availability of ~~all~~the electronic protected health information ~~the covered entity or business associate creates, receives, maintains, or transmits~~.

(2) Protect against any reasonably anticipated threats or hazards to the ~~security or~~confidentiality, integrity, or availability of ~~such~~the electronic protected health information.

(3) Protect against any reasonably anticipated uses or disclosures of ~~such~~the electronic protected health information that are not permitted or required under subpart E of this part.

(4) Ensure compliance by its workforce with this subpart ~~by its workforce~~and all administrative, physical, and technical safeguards implemented in accordance with this subpart.

(b) *Flexibility of approach.*

(1) Covered entities and business associates may use any reasonable and appropriate security measures that allow the covered entity or business associate 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 or business associate must take into account all of the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate'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.

(v) The effectiveness of the security measure in supporting the resiliency of the covered entity or business associate.

(c) *Standards.* *and implementation specifications.* A covered entity or business associate must comply with the applicable standards, including their implementation specifications, as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314 and 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 § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate 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 electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(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.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with ~~§~~ §§ 164.306~~:~~

~~(1)~~

~~(i) *Standard: Security management process.* Implement policies~~ and ~~procedures~~164.316, implement all of the following administrative safeguards to ~~prevent, detect, contain~~protect the confidentiality, integrity, and ~~correct security violations.~~availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(1) *Standard: Technology asset inventory* —

(i) *General.* Conduct and maintain an accurate and thorough written inventory and a network map of the covered entity's or business associate's electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of electronic protected health information.

(ii) *Implementation specifications~~:~~* —

(A) *Inventory.* Develop a written inventory of the covered entity's or business associate's technology assets that contains the identification, version, person accountable, and location of each technology asset.

(B) *Network map.* Develop a network map that illustrates the movement of electronic protected health information throughout the covered entity's or business associate's electronic information systems, including but not limited to how electronic protected health information enters and exits such information systems, and is accessed from outside of such information systems.

(C) *Maintenance.* Review and update the written inventory of technology assets required by paragraph (a)(1)(ii)(A) of this section and the network map required by paragraph (a)(1)(ii)(B) of this section in the following circumstances:

$(1) On an ongoing basis, but at least once every 12 months.

$(2) When there is a change in the covered entity's or business associate's environment or operations that may affect electronic protected health information, including but not limited to the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of electronic protected health information; a sale, transfer, merger, or consolidation of all or part of the covered entity or business associate with another person; a security incident that affects the confidentiality, integrity, and availability of electronic protected health information; and relevant changes in Federal, State, Tribal, or territorial law.

(2) *Standard:* *Risk analysis* ~~*(Required).*~~ —

(i) *General.* Conduct an accurate and ~~thorough~~comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information ~~held~~created, received, maintained, or transmitted by the covered entity or business associate.

(ii) *Implementation specifications —*

(A) *Assessment.* The written assessment must include, at a minimum, all of the following:

$(*1*) A review of the technology asset inventory required by paragraph (a)(1)(ii)(A) of this section and the network map required by paragraph (a)(1)(ii)(B) of this section to identify where electronic protected health information may be created, received, maintained, or transmitted within the covered entity's or business associate's electronic information systems.

$(*2*) Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits.

$(*3*) Identification of potential vulnerabilities and predisposing conditions to the covered entity's or business associate's relevant electronic information systems.

$(*4*) An assessment and documentation of the security measures the covered entity or business associate uses to ensure the confidentiality, integrity, and availability of the electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

$(*5*) A reasonable determination of the likelihood that each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section will exploit the vulnerabilities identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section.

$(*6*) A reasonable determination of the potential impact of each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section successfully exploiting the vulnerabilities identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section.

$(*7*) An assessment of risk level for each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section and vulnerability identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section, based on the determinations made in accordance with paragraphs (a)(2)(ii)(A)(*5*) and (*6*) of this section.

$(*8*) An assessment of the risks to electronic protected health information posed by entering into or continuing a business associate contract or other written arrangement with any prospective or current business associate, respectively, based on the written verification obtained from the prospective or current business associate in accordance with paragraph (b)(1) of this section.

(B) *Maintenance.* Review, verify, and update the written assessment on an ongoing basis, but at least once every 12 months and, in accordance with paragraph (a)(1)(ii)(C)(*2*) of this section, in response to a change in the covered entity's or business associate's environment or operations that may affect electronic protected health information.

(3) *Standard: Evaluation —*

(i) *General.* Perform a written technical and nontechnical evaluation to determine whether a change in the covered entity's or business associate's environment or operations may affect the confidentiality, integrity, or availability of electronic protected health information.

(ii) *Implementation specifications —*

(A) *Performance.* Perform a written technical and nontechnical evaluation within a reasonable period of time before making a change in the covered entity's or business associate's environment or operations as described in paragraph (a)(1)(ii)(C)(*2*) of this section.

(B) *Response.* Respond to the written technical and nontechnical evaluation in accordance with the covered entity's or business associate's risk management plan required by paragraph (a)(5)(ii)(A) of this section.

(4) *Standard: Patch management —*

(i) *General.* Implement written policies and procedures for applying patches and updating the configuration(s) of the covered entity's or business associate's relevant electronic information systems.

(ii) *Implementation specifications —*

(A) *Policies and procedures.* Establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout the covered entity's or business associate's relevant electronic information systems.

(B) *Maintenance.* Review and test written policies and procedures required by paragraph (a)(4)(ii)(A) of this section at least once every 12 months, and modify such policies and procedures as reasonable and appropriate.

(C) *Application.* Patch, update, and upgrade the configurations of relevant electronic information systems in accordance with the written policies and procedures required by paragraph (a)(4)(ii)(A) of this section and based on the results of the covered entity's or business associate's risk analysis required by paragraph (a)(2) of this section, the vulnerability scans required by § 164.312(h)(2)(i), the monitoring of authoritative sources required by § 164.312(h)(2)(ii), and penetration tests required by § 164.312(h)(2)(iii), within a reasonable and appropriate period of time, as follows, except to the extent that an exception at paragraph (a)(4)(ii)(D) of this section applies:

$(*1*) Within 15 calendar days of identifying the need to patch, update, or upgrade the configuration of a relevant electronic information system to address a critical risk in accordance with this paragraph (a)(4)(ii)(C), where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 15 calendar days of a patch, update, or upgrade becoming available.

$(2) Within 30 calendar days of identifying the need to patch, update, or upgrade the configuration of a relevant electronic information system to address a high risk in accordance with this paragraph (a)(4)(ii)(C), where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 30 calendar days of a patch, update, or upgrade becoming available.

$(*3*) As determined by and documented in the covered entity's or business associate's policies and procedures under paragraph (a)(4)(ii)(A) of this section for all other patches, updates, and upgrades to the configuration of a relevant electronic information system.

(D) *Exceptions.* This paragraph (a)(4)(ii)(D) applies only to the extent that a covered entity or business associate documents that an exception in this paragraph (a)(4)(ii)(D) applies and that all other applicable conditions are met.

$(*1*) A patch, update, or upgrade to the configuration of a relevant electronic information system is not available to address a risk identified in the risk analysis under paragraph (a)(2) of this section.

$(2) The only available patch, update, or upgrade would adversely affect the confidentiality, integrity, or availability of electronic protected health information.

(E) *Alternative measures.* Where an exception at paragraph (a)(4)(ii)(D) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (a)(4)(ii)(F) of this section.

(F) *Compensating controls.* To the extent that a covered entity or business associate determines that an exception at paragraph (a)(4)(ii)(D) of this section applies, a covered entity or business associate must implement reasonable and appropriate security measures to address the identified risk in a timely manner as required by paragraph (a)(5)(ii)(D) of this section until a patch, update, or upgrade that does not adversely affect the confidentiality, integrity, or availability of electronic protected health information becomes available.

(5) *Standard:* *Risk management* ~~*(Required).*~~ —

(i) *General.* Implement security measures sufficient to reduce risks and vulnerabilities to all electronic protected health information to a reasonable and appropriate level ~~to comply with § 164.306(a).~~.

~~(C)~~(ii) *Implementation specifications* —

(A) *Planning.* Establish and implement a written risk management plan for reducing risks to all electronic protected health information, including but not limited to those risks identified by the risk analysis under paragraph (a)(2)(ii)(A) of this section, to a reasonable and appropriate level.

(B) *Maintenance.* Review the written risk management plan required by paragraph (a)(5)(ii)(A) of this section at least once every 12 months and as reasonable and appropriate in response to changes in the risk analysis made in accordance with paragraph (a)(2)(ii)(B) of this section, and modify as reasonable and appropriate.

(C) *Priorities.* The written risk management plan must prioritize the risks identified in the risk analysis required by paragraph (a)(2)(ii)(A) of this section, based on the risk levels determined by such risk analysis.

(D) *Implementation.* Implement security measures in a timely manner to address the risks identified in the covered entity's or business associate's risk analysis in accordance with the priorities established under paragraph (a)(5)(ii)(C) of this section.

(6) *Standard:* *Sanction policy* ~~*(Required).*~~ —

(i) *General.* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

~~(D)~~ (ii) *Implementation specifications* —

(A) *Policies and procedures.* Establish written policies and procedures for sanctioning workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(B) *Modifications.* Review written sanctions policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

(C) *Application.* Apply and document appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate in accordance with the written policies and procedures for sanctioning workforce members required by paragraph (a)(6)(ii)(A) of this section.

(7) *Standard:* *Information system activity review* ~~*(Required).*~~ —

(i) *General.* Implement written policies and procedures ~~to~~for regularly ~~review~~reviewing records of activity in the covered entity's or business associate's relevant electronic information ~~system activity,~~systems.

(ii) *Implementation specifications* —

(A) *Policies and procedures.* Establish written policies and procedures for retaining and reviewing records of activity in the covered entity's or business associate's relevant electronic information systems by persons and technology assets, including the frequency for reviewing such ~~as~~ records.

(B) *Scope.* Records of activity in the covered entity's or business associate's relevant electronic information systems by persons and/or technology assets include but are not limited to audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports.

~~(2~~(C) *Record review.* Review records of activity in a covered entity's or business associate's relevant electronic information systems by persons and technology assets as often as reasonable and appropriate for the type of report or log and document such review.

(D) *Record retention.* Retain records of activity in the covered entity's or business associate's relevant electronic information systems by persons and technology assets for a period of time that is reasonable and appropriate for the type of report or log.

(E) *Response.* Where a suspected or known security incident is identified during the review required by paragraph (a)(7)(ii)(C) of this section, respond in accordance with the covered entity's or business associate's security incident response plan required by paragraph (a)(12)(ii)(A)(*1*) of this section.

(F) *Maintenance.* Review and test the written policies and procedures required by paragraph (a)(7)(ii)(A) of this section at least once every 12 months and modify as reasonable and appropriate.

(8) *Standard: Assigned security responsibility.* ~~Identify~~In writing, identify the security official who is responsible for the development and implementation of the policies and procedures, written or otherwise, and deployment of technical controls required by this subpart for the covered entity or business associate.

~~covered entity or business associate~~

~~(3)~~

~~(i~~(9) *Standard: Workforce security* —

(i) *General*. Implement written 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 relevant electronic information systems, and to prevent those workforce members who ~~do~~are not authorized to have access ~~under paragraph (a)(4) of this section~~ from obtaining access to electronic protected health information~~.~~ and relevant electronic information systems.

(ii) *Implementation specifications*~~:~~ —

(A) *Authorization and/or supervision ~~(Addressable).~~* ~~Implement~~. Establish and implement written procedures for the authorization and/or supervision of workforce members who ~~work with~~access electronic protected health information or relevant electronic information systems, or who work in ~~locations~~facilities where ~~it~~electronic protected health information or relevant electronic information systems might be accessed.

(B) *Workforce clearance procedure ~~(Addressable).~~* ~~Implement~~. Establish and implement written procedures to determine that the access of a workforce member to electronic protected health information ~~is appropriate.~~or relevant electronic information systems is appropriate in accordance with paragraph (a)(10)(ii)(B) of this section.

(C) ~~*Termination*~~*Modification and termination procedures ~~(Addressable).~~* ~~Implement~~.

$(*1*) Establish and implement written procedures ~~for terminating access~~, in accordance with paragraph (a)(9)(ii)(C)(2) of this section, to terminate a workforce member's access to electronic protected health information ~~when~~and relevant electronic information systems, and to facilities where electronic protected health information or relevant electronic information systems might be accessed.

$(2) A workforce member's access must be terminated as soon as possible but no later than one hour after the employment of, or other arrangement with, a workforce member ends ~~or as~~.

(D) *Notification.*

$(*1*) Establish and implement written procedures, in accordance with paragraph (a)(9)(ii)(D)(2) of this section, to notify another covered entity or business associate of a change in or termination of access where the workforce member is or was authorized to access such electronic protected health information or relevant electronic information systems by the covered entity or business associate making the notification.

$(2) Notification must occur as soon as possible but no later than 24 hours after a change in or termination of a workforce member's authorization to access electronic protected health information or relevant electronic information systems maintained by such other covered entity or business associate.

(E) *Maintenance.* Review and test written policies and procedures required ~~by determinations made as specified in~~under paragraph (a)(~~3~~9)(ii)(~~B~~A) through (D) of this section~~.~~ at least once every 12 months, and modify as reasonable and appropriate.

~~(4)~~

~~(i~~(10) *Standard: Information access management*~~. Implement~~ —

(i) *General.* Establish and implement written policies and procedures for authorizing access to electronic protected health information and relevant electronic information systems 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 establish and implement written policies and procedures that protect the electronic protected health information and relevant electronic information systems of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization* ~~*(Addressable).* Implement~~. Establish and implement written policies and procedures for granting and revising access to electronic protected health information~~,~~ and relevant electronic information systems as necessary and appropriate for each prospective user and technology asset to carry out their assigned function(s).

(C) *Authentication management.* Establish and implement written policies and procedures for ~~example, through access to a workstation, transaction, program, process, or other mechanism.~~verifying the identities of users and technology assets prior to accessing the covered entity's or business associate's relevant electronic information systems, including written policies and procedures for implementing multi-factor authentication technical controls required by § 164.312(f)(2)(ii) through (v).

~~(C~~(D) *Access* ~~*establishment*~~*determination and modification* ~~*(Addressable).* Implement~~. Establish and implement written policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, ~~establish~~determine, document, review, and modify ~~a user's right of~~ the access of each user and technology asset to ~~a workstation, transaction, program,~~specific components of the covered entity's or ~~process.~~business associate's relevant electronic information systems.

~~(5)~~

~~(i~~(E) *Network segmentation.* Establish and implement written policies and procedures that ensure that a covered entity's or business associate's relevant electronic information systems are segmented to limit access to electronic protected health information to authorized workstations.

(F) *Maintenance.* Review and test the written policies and procedures required by this paragraph (a)(10)(ii) at least once every 12 months, and modify as reasonable and appropriate.

(11) *Standard: Security awareness ~~and~~ training* —

(i) *General*. Implement ~~a~~ security awareness ~~and~~ training ~~program~~ for all workforce members ~~of its workforce (including management).~~on protection of electronic protected health information and information systems as necessary and appropriate for the members of the workforce to carry out their assigned function(s).

(ii) *Implementation specifications*~~. Implement:~~ —

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

~~(B) *Protection from malicious software (Addressable).* Procedures for guarding~~(A) *Training.* A covered entity or business associate must develop and implement security awareness training for all workforce members that addresses all of the following:

$(*1*) The written policies and procedures with respect to electronic protected health information required by this subpart as necessary and appropriate for the workforce members to carry out their assigned functions.

$(2) Guarding against, detecting, and reporting suspected or known security incidents, including but not limited to, malicious software and social engineering.

$(*3*) The written policies and procedures for accessing the covered entity's or business associate's relevant electronic information systems, including but not limited to: safeguarding passwords; setting unique passwords of sufficient strength to ensure the confidentiality, integrity, and availability of electronic protected health information; and limitations on sharing passwords.

(B) *Timing.* A covered entity or business associate must provide security awareness training as follows:

$(*1*) As required by paragraph (a)(11)(ii)(A) of this section, to each member of its workforce by no later than the compliance date, and at least once every 12 months thereafter.

$(2) As required by paragraph (a)(11)(ii)(A) of this section, to each new member of its workforce within a reasonable period of time but no later than 30 days after the person first has access to the covered entity's or business associate's relevant electronic information systems.

$(*3*) On a material change to the policies or procedures required by this subpart, to each member of its workforce whose functions are affected by such change, within a reasonable period of time but no later than 30 days after the material change occurs.

(C) *Ongoing education.* A covered entity or business associate must provide its workforce members ongoing reminders of their security responsibilities and notifications of relevant threats, including but not limited to new and emerging malicious software~~.~~ and social engineering.

~~(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~~(D) *Documentation.* A covered entity or business associate must document that the training required by paragraph (a)(11)(ii)(A) of this section and ongoing reminders required by paragraph (a)(11)(ii)(C) of this section have been provided.

(12) *Standard: Security incident procedures~~.~~* —

(i) *General.* Implement written policies and procedures to respond to security incidents.

(ii) *Implementation specifications* —

(A) *Planning and testing.*

$(*1*) Establish written security incident response plan(s) and procedures documenting how workforce members are to report suspected or known security incidents and how the covered entity or business associate will respond to suspected or known security incidents in accordance with paragraph (a)(12)(ii)(B) of this section.

$(2) Implement ~~policies and~~written procedures ~~to address~~for testing and revising security ~~incidents.~~incident response plan(s) required by paragraph (a)(12)(ii)(A)(*1*) of this section.

~~(ii) *Implementation specification:*~~$(*3*) Review and test security incident response plan(s) and procedures required by paragraph (a)(12)(ii)(A)(*1*) of this section at least once every 12 months, document the results of such tests, and modify security incident response plan(s) and procedures as reasonable and appropriate.

(B) *Response~~ and reporting (Required).~~*

$(*1*) Identify and respond to suspected or known security incidents~~; mitigate~~.

$(2) Mitigate, to the extent practicable, harmful effects of security incidents that are suspected or known to the covered entity or business associate~~; and document security incidents and their outcomes.~~.

~~(7)~~

~~(i~~$(*3*) Identify and remediate, to the extent practicable, the root cause(s) of security incidents that are suspected or known to the covered entity or business associate.

$(*4*) Eradicate the security incidents that are suspected or known to the covered entity or business associate.

$(*5*) For suspected and known security incidents, develop and maintain documentation of investigations, analyses, mitigation, and remediation.

(13) *Standard: Contingency plan* —

(i) *General*. Establish ~~(~~and implement as needed~~)~~ a written contingency plan, consisting of written policies and procedures for responding to an emergency or other occurrence ~~(for example,~~ —including but not limited to fire, vandalism, system failure, ~~and~~ natural disaster~~)~~, or security incident—that ~~damages systems that contain~~adversely affects relevant electronic ~~protected health~~ information~~.~~ systems.

(ii) *Implementation specifications~~:~~* —

~~(A~~(A) *Criticality analysis.* Perform and document an assessment of the relative criticality of the covered entity's or business associate's relevant electronic information systems and technology assets in its relevant electronic information systems.

(B) *Data ~~backup plan (Required).~~ backups.* Establish and implement written procedures to create and maintain exact retrievable ~~exact~~ copies of electronic protected health information~~.~~, including verification that the electronic protected health information has been copied accurately.

~~(B~~(C) *Information systems backups.* Establish and implement written procedures to create and maintain backups of the covered entity's or business associate's relevant electronic information systems, including verification of success of backups.

(D) *Disaster recovery plan ~~(Required).~~*

$(*1*) Establish (and implement as needed) written procedures to restore ~~any~~ loss of the covered entity's or business associate's critical relevant electronic information systems and data~~.~~ within 72 hours of the loss.

~~(C) *Emergency mode operation plan (Required).* Establish (and implement as needed)~~$(*2*) Establish (and implement as needed) written procedures to restore loss of the covered entity's or business associate's other relevant electronic information systems and data in accordance with the criticality analysis required by paragraph (a)(13)(ii)(A) of this section.

(E) *Emergency mode operation plan.* Establish (and implement as needed) written procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

~~(D~~(F) *Testing and revision procedures ~~(Addressable).~~* ~~Implement~~.

$(*1*) Establish written procedures for ~~periodic~~ testing and ~~revision of~~revising contingency plans~~.~~ as required by this paragraph (a)(13) in accordance with paragraph (a)(13)(ii)(F)(2) of this section.

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

~~(8~~$(2) Review and test contingency plans required by this paragraph (a)(13) at least once every 12 months, document the results of such tests, and modify such contingency plans as reasonable and appropriate in accordance with the results of those tests.

(14) *Standard: ~~Evaluation.~~ Compliance audit.* Perform ~~a periodic 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~~ document an audit at least once every 12 months of ~~electronic protected health information, that establishes the extent to which a~~the covered entity's or business associate's ~~security policies~~compliance with each standard and ~~procedures meet the requirements of~~implementation specification in this subpart.

(b)

(1) *Standard:* *Business associate contracts and other arrangements.*

(i)

(A) A covered entity 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 ~~§~~ § 164.314(a), that the business associate will ~~appropriately safeguard~~ comply with this subpart and verifies that the ~~information. A covered entity is not required to obtain such satisfactory assurances from a~~ business associate ~~that is a subcontractor.~~has deployed technical safeguards in accordance with the requirements of § 164.312.

~~(2~~(B) A covered entity is not required to obtain such satisfactory assurances or verification from a business associate that is a subcontractor.

(ii) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with ~~§~~ § 164.314(a), that the subcontractor will ~~appropriately safeguard~~comply with the ~~information~~requirements of this subpart and verifies that the business associate that is a subcontractor has deployed technical safeguards in accordance with the requirements of § 164.312.

~~(3~~(2) *Implementation specifications:* —

(i) *Written contract or other arrangement ~~(Required).~~* Document the satisfactory assurances required by paragraph (b)(1)(i) or (~~b)(2~~ii) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of ~~§~~ § 164.314(a).

(ii) *Written verification.* Obtain written verification from the business associate at least once every 12 months that the business associate has deployed the technical safeguards as required by § 164.312 through both of the following:

(A) A written analysis of the business associate's relevant electronic information systems by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information to verify compliance with each standard and implementation specification in § 164.312.

(B) A written certification that the analysis has been performed and is accurate by a person who has the authority to act on behalf of the business associate.

(3) *Standard: Delegation to business associate.*

(i) A covered entity or business associate may permit a business associate to serve as their designated security official.

(ii) A covered entity or business associate that delegates actions, activities, or assessments required by this subpart to a business associate remains liable for compliance with all applicable provisions of this subpart.

164.310 Physical safeguards.

~~A~~Each covered entity ~~or~~and business associate must, in accordance with ~~§~~ §§ 164.306 and 164.316, implement all of the following physical safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(a)

~~(1)~~ *Standard: Facility access controls*~~. Implement~~ —

(1) *General.* Establish and implement written policies and procedures to limit physical access to all of its relevant 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* ~~*(Addressable).*~~ Establish (and implement as needed) written procedures that allow facility access in support of ~~restoration of lost data under the disaster recovery~~the covered entity's or business associate's contingency plan ~~and emergency mode operations plan in the event of an emergency~~ required by § 164.308(a)(13).

(ii) *Facility security plan* ~~*(Addressable).* Implement~~. Establish and implement written policies and procedures to safeguard ~~the facility~~ all facilities and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access* ~~*control*~~*management and validation procedures* ~~*(Addressable).* Implement~~. Establish and implement written procedures to ~~control~~authorize and ~~validate~~manage 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.~~management.

(iv) ~~*Maintenance*~~*Physical maintenance records* ~~*(Addressable).* Implement~~. Establish and implement written policies and procedures to document repairs and modifications to the physical components of a facility ~~which~~that are related to security ~~(for example,~~, including but not limited to hardware, walls, doors, ~~and~~ locks~~)~~., and security cameras.

(v) *Maintenance.* For each facility, review and test the written policies and procedures required by this paragraph (a)(2) at least once every 12 months, and modify such policies and procedures as reasonable and appropriate.

(b) *Standard: Workstation use*~~. Implement~~ —

(1) *General.* Establish and implement written policies and procedures that govern the use of workstations that access electronic protected health information or the covered entity's or business associate's relevant electronic information systems.

(2) *Implementation specifications* —

(i) *Policies and procedures.* The written policies and procedures must specify ~~the proper~~all of the following with respect to a workstation that accesses electronic protected health information or the covered entity's or business associate's relevant electronic information systems:

(A) The functions ~~to~~ for which a workstation may be ~~performed, the~~ used.

(B) The manner in which a workstation may be used to perform those functions ~~are to be performed, and the~~.

(C) The physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information, including the removal of such workstations from a facility and the movement of such workstations within and outside of a facility.

(ii) *Maintenance.* Review and test written policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

(c) *Standard: Workstation security.* Implement and modify physical safeguards for all workstations that access electronic protected health information or relevant electronic information systems, to address the written policies and procedures for workstation use required by paragraph (b) of this section and restrict access to authorized users.

(d)

~~(1)~~ *Standard: ~~Device and media~~Technology asset controls*~~. Implement~~ —

(1) *General.* Establish and implement written policies and procedures that govern the receipt and removal of ~~hardware and electronic media~~technology assets that ~~contain~~maintain electronic protected health information into and out of a facility, and the movement of these ~~items~~assets within the facility.

(2) *Implementation specifications*~~:~~ —

(i) *Disposal ~~(Required).~~* ~~Implement~~. Establish and implement written policies and procedures ~~to address the final disposition~~for disposal of electronic protected health information~~,~~ and~~/or~~ the ~~hardware or electronic media~~technology assets on which it is ~~stored.~~maintained based on current standards for disposing of such technology assets.

(ii) *Media ~~re-use (Required).~~* ~~Implement~~*sanitization.* Establish and implement written procedures for removal of electronic protected health information from electronic media such that the electronic protected health information cannot be recovered, based on current standards for sanitizing 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.~~

(iii) *Maintenance.* Review and test the written policies and procedures required by paragraphs (d)(2)(i) and (ii) of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

164.312 Technical safeguards.

~~A~~Each covered entity or business associate must, in accordance with ~~§~~ §§ 164.306 and 164.316, implement all of the following technical safeguards, including technical controls, to protect the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(a)

~~(1)~~ *Standard: Access control*~~. Implement~~ —

(1) *General.* Deploy technical ~~policies and procedures for~~controls in relevant electronic information systems ~~that maintain electronic protected health information~~ to allow access only to ~~those persons or software programs~~users and technology assets that have been granted access rights ~~as specified in § 164.308(a)(4).~~.

(2) *Implementation specifications*~~:~~ —

(i) *Unique ~~user~~ identification ~~(Required).~~*. Assign a unique name, number, and/or ~~number~~other identifier for ~~identifying and~~ tracking ~~user identity.~~each user and technology asset in the covered entity or business associate's relevant electronic information systems.

(ii) *Administrative and increased access privileges.* Separate user identities from identities used for administrative and other increased access privileges.

(iii) *Emergency access procedure ~~(Required).~~*. Establish (and implement as needed) written and technical procedures for obtaining necessary electronic protected health information during an emergency.

~~(iii~~(iv) *Automatic logoff ~~(Addressable).~~ ~~Implement electronic procedures~~*. Deploy technical controls that terminate an electronic session after a predetermined time of inactivity~~.~~ that is reasonable and appropriate.

~~(iv)~~ (v) *Log-in attempts.* Deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a reasonable and appropriate predetermined number of unsuccessful authentication attempts.

(vi) *Network segmentation.* Deploy technical controls to ensure that the covered entity's or business associate's relevant electronic information systems are segmented in a reasonable and appropriate manner.

(vii) *Data controls.* Deploy technical controls to allow access to electronic protected health information only to those users and technology assets that have been granted access rights to the covered entity's or business associate's relevant electronic information systems as specified in § 164.308(a)(10).

(viii) *Maintenance.* Review and test the effectiveness of the procedures and technical controls required by this paragraph (a)(2) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(b) *Standard:* *Encryption and decryption* ~~*(Addressable).* Implement a mechanism~~

(1) *General.* Deploy technical controls to encrypt and decrypt electronic protected health information~~.~~ using encryption that meets prevailing cryptographic standards.

(2) *Implementation specification.* Encrypt all electronic protected health information at rest and in transit, except to the extent that an exception at paragraph (b)(3) of this section applies.

(3) *Exceptions.* This paragraph (b)(3) applies only to the electronic protected health information directly affected by one or more of the following exceptions and only to the extent that the covered entity or business associate documents that an exception applies and that all other applicable conditions are met.

(i) The technology asset in use does not support encryption of the electronic protected health information consistent with prevailing cryptographic standards, and the covered entity or business associate establishes and implements a written plan to migrate electronic protected health information to a technology asset that supports encryption consistent with prevailing cryptographic standards within a reasonable and appropriate period of time.

(ii) An individual requests pursuant to § 164.524 to receive their electronic protected health information in an unencrypted manner and has been informed of the risks associated with the transmission, receipt, and storage of unencrypted electronic protected health information. This exception does not apply where such individual will receive their electronic protected health information pursuant to § 164.524 and the technology used by the individual to receive the electronic protected health information is controlled by the covered entity or its business associate.

(iii) During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems in which encryption is infeasible, and the covered entity or business associate implements reasonable and appropriate compensating controls in accordance with and determined by the covered entity's or business associate's contingency plan under § 164.308(a)(13).

(iv) The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration, as follows:

(A) Pursuant to a submission received before March 29, 2023, provided that the covered entity or business associate deploys in a timely manner any updates or patches required or recommended by the manufacturer of the device.

(B) Pursuant to a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

(C) Pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer.

(4) *Alternative measures —*

(i) *Alternative measures.* Where an exception at paragraph (b)(3) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (b)(4)(ii) of this section.

(ii) *Compensating controls.*

(A) To the extent that a covered entity or business associate determines that an exception at paragraph (b)(3)(i), (ii), or (iii) or (b)(3)(iv)(A) or (B) of this section applies, the covered entity or business associate must secure such electronic protected health information by implementing reasonable and appropriate compensating controls reviewed and approved by the covered entity's or business associate's designated Security Official.

(B) To the extent that a covered entity or business associate determines that an exception at paragraph (b)(3)(iv)(C) of this section applies, the covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.

(C) To the extent that a covered entity or business associate is implementing compensating controls under this paragraph (b)(4)(ii), the implementation and effectiveness of compensating controls must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, to continue securing electronic protected health information and relevant electronic information systems.

(5) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (b) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(c) *Standard: Configuration management —*

(1) *General.* Establish and deploy technical controls for securing the covered entity's or business associate's relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner, and maintain such electronic information systems and technology assets according to the covered entity's or business associate's established secure baselines.

(2) *Implementation specifications —*

(i) *Anti-malware protection.* Deploy technology assets and/or technical controls that protect all of the covered entity's or business associate's technology assets in its relevant electronic information systems against malicious software, including but not limited to viruses and ransomware.

(ii) *Software removal.* Remove extraneous software from the covered entity's or business associate's relevant electronic information systems.

(iii) *Configuration.* Configure and secure operating system(s) and software consistent with the covered entity's or business associate's risk analysis under § 164.308(a)(2).

(iv) *Network ports.* Disable network ports in accordance with the covered entity's or business associate's risk analysis under § 164.308(a)(2).

(v) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (c) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(d) *Standard: Audit trail and system log controls*~~. Implement hardware, software,~~ —

(1) *General.* Deploy technology assets and/or ~~procedural mechanisms~~technical controls that record and ~~examine~~identify activity in the covered entity's or business associate's relevant electronic information systems~~ that contain or use electronic protected health information.~~.

~~(c)~~

~~(1) *Standard: Integrity.* Implement~~(2) *Implementation specifications* —(i) *Monitor and identify.* The covered entity or business associate must deploy technology assets and/or technical controls that monitor in real-time all activity in its relevant electronic information systems, identify indications of unauthorized persons or unauthorized activity as determined by the covered entity's or business associate's risk analysis under § 164.308(a)(2), and alert workforce members of such indications in accordance with the policies and procedures required by § 164.308(a)(7).

(ii) *Record.* The covered entity or business associate must deploy technology assets and/or technical controls that record in real-time all activity in its relevant electronic information systems.

(iii) *Retain.* The covered entity or business associate must deploy technology assets and/or technical controls to retain records of all activity in its relevant electronic information systems as determined by the covered entity's or business associate's policies and procedures for information system activity review at § 164.308(a)(7)(ii)(A).

(iv) *Scope.* Activity includes creating, accessing, receiving, transmitting, modifying, copying, or deleting any of the following:

(A) Electronic protected health information.

(B) Relevant electronic information systems and the information therein.

(v) *Maintenance.* Review and test the effectiveness of the technology assets and/or technical controls required by this paragraph (d) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(e) *Standard: Integrity.* Deploy technical controls to protect electronic protected health information from improper alteration or destruction~~.~~, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

~~(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.~~

~~(~~d(f) *Standard: ~~Person or entity authentication.~~* Implement procedures*Authentication —*

(1) *General.* Deploy technical controls to verify that a person or ~~entity~~ technology asset seeking access to electronic protected health information and/or the covered entity's or business associate's relevant electronic information systems is the one claimed.

~~(e)~~

~~(1)~~ (2) *Implementation specifications —*

(i) *Information access management policies.* Deploy technical controls in accordance with the covered entity's or business associate's information access management policies and procedures under § 164.308(a)(10), including technical controls that require users to adopt unique passwords that are consistent with the current recommendations of authoritative sources.

(ii) *Multi-factor authentication.* (A) Deploy multi-factor authentication to all technology assets in the covered entity's or business associate's relevant electronic information systems to verify that a person seeking access to the relevant electronic information system(s) is the user that the person claims to be.

(B) Deploy multi-factor authentication for any action that would change a user's privileges to the covered entity's or business associate's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of electronic protected health information.

(iii) *Exceptions.* Deployment of multi-factor authentication is not required in any of the following circumstances.

(A) The technology asset in use does not support multi-factor authentication, and the covered entity or business associate establishes and implements a written plan to migrate electronic protected health information to a technology asset that supports multi-factor authentication within a reasonable and appropriate period of time.

(B) During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems or the confidentiality, integrity, or availability of electronic protected health information in which multi-factor authentication is infeasible and the covered entity or business associate implements reasonable and appropriate compensating controls in accordance with its emergency access procedures under paragraph (a)(2)(iii) of this section and the covered entity's or business associate's contingency plan under § 164.308(a)(13).

(C) The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration, as follows:

$(*1*) Pursuant to a submission received before March 29, 2023, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

$(2) Pursuant to a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

$(3) Pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer.

(iv) *Alternative measures —*

(A) *Alternative measures.* Where an exception at paragraph (f)(2)(iii) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls as required by paragraph (f)(2)(iv)(B) of this section.

(B) *Compensating controls.*

$(1) To the extent that a covered entity or business associate determines that an exception at paragraph (f)(2)(iii)(A) or (B) or (f)(2)(iii)(C)(1) or (2) of this section applies, the covered entity or business associate must secure its relevant electronic information systems by implementing reasonable and appropriate compensating controls reviewed, approved, and signed by the covered entity's or business associate's designated Security Official.

$(2) To the extent that a covered entity or business associate determines that an exception at paragraph (f)(2)(iii)(C)(3) of this section applies, the covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.

$(3) To the extent that a covered entity or business associate is implementing compensating controls under this paragraph (f)(2)(iv)(B), the effectiveness of compensating controls must be reviewed and documented by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, to continue securing electronic protected health information and its relevant electronic information systems.

(v) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (f) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(g) *Standard: Transmission security.* ~~Implement~~Deploy technical ~~security measures~~controls to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network~~.~~; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(h) *Standard: Vulnerability management —*

(1) *General.* Deploy technical controls in accordance with the covered entity's or business associate's patch management policies and procedures required by § 164.308(a)(4)(ii)(A) to identify and address technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems.

(2) *Implementation specifications*~~:~~ —

(i) ~~*Integrity controls (Addressable).* Implement security measures to ensure~~ *Vulnerability scanning.*

(A) Conduct automated vulnerability scans to identify technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems in accordance with the covered entity's or business associate's risk analysis required by § 164.308(a)(2) or at least once every six months, whichever is more frequent.

(B) Review and test the effectiveness of the technology asset(s) that ~~electronically transmitted~~conducts the automated vulnerability scans required by paragraph (h)(2)(i)(A) of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(ii) *Monitoring.* Monitor authoritative sources for known vulnerabilities on an ongoing basis and remediate such vulnerabilities in accordance with the covered entity's or business associate's patch management program under § 164.308(a)(4).

(iii) *Penetration testing.* Perform penetration testing of the covered entity's or business associate's relevant electronic information systems by a qualified person.

(A) A qualified person is a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information ~~is not improperly modified without detection until disposed of~~.

~~(ii) *Encryption (Addressable).* Implement a mechanism to encrypt~~(B) Penetration testing must be performed at least once every 12 months or in accordance with the covered entity's or business associate's risk analysis required by § 164.308(a)(2), whichever is more frequent.

(iv) *Patch and update installation.* Deploy technical controls in accordance with the covered entity's or business associate's patch management program under § 164.308(a)(4) to ensure timely installation of software patches and critical updates as reasonable and appropriate.

(i) *Standard: Data backup and recovery* —

(1) *General.* Deploy technical controls to create and maintain exact retrievable copies of electronic protected health information ~~whenever deemed appropriate.~~.

(2) *Implementation specifications* —

(i) *Data backup.* Create backups of electronic protected health information in accordance with the policies and procedures required by § 164.308(a)(13)(ii)(B) and with such frequency to ensure retrievable copies of electronic protected health information are no more than 48 hours older than the electronic protected health information maintained in the covered entity or business associate's relevant electronic information systems.

(ii) *Monitor and identify.* Deploy technical controls that, in real-time, monitor, and alert workforce members about, any failures and error conditions of the backups required by paragraph (i)(2)(i) of this section.

(iii) *Record.* Deploy technical controls that record the success, failure, and any error conditions of backups required by paragraph (i)(2)(i) of this section.

(iv) *Testing.* Restore a representative sample of electronic protected health information backed up as required by paragraph (i)(2)(i) of this section, and document the results of such test restorations at least monthly.

(j) *Standard: Information systems backup and recovery.* Deploy technical controls to create and maintain backups of relevant electronic information systems; and review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

164.314 Organizational requirements.

(a)

(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by ~~§~~ § 164.308(b)(~~3~~2) must meet the requirements of paragraph (a)(2)(i), (~~a)(2)(~~ii), or (~~a)(2)(~~iii) of this section, as applicable.

(2) *Implementation specifications ~~(Required)~~* —

(i) *Business associate contracts.* The contract must provide that the business associate will~~—~~ do all of the following:

(A) Comply with the applicable requirements of this subpart~~;~~.

(B) In accordance with ~~§~~ § 164.308(b)(~~2~~1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section~~; and~~.

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured electronic protected health information as required by ~~§~~ § 164.410.

(D) Report to the covered entity activation of its contingency plan under § 164.308(a)(13) without unreasonable delay, and in no case later than 24 hours after activation of the contingency plan.

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of ~~§~~ § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (~~a)(2)(~~ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by ~~§~~ § 164.308(b)(~~4~~1)(ii) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)

(1) *Standard: Requirements for group health plans.* Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to ~~§~~ § 164.504(f)(1)(ii) or (iii), or as authorized under ~~§~~ § 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~~—~~ do all of the following:

(i) *Safeguard implementation.* Implement the administrative, physical, and technical safeguards that ~~reasonably~~covered entities and ~~appropriately protect the confidentiality, integrity~~business associates are required to implement under §§ 164.308(a), 164.310, and ~~availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;~~164.312.

(ii) *Separation.* Ensure that the adequate separation required by ~~§~~ § 164.504(f)(2)(iii) is supported by ~~reasonable~~the administrative, physical, and ~~appropriate security measures;~~technical safeguards implemented in accordance with paragraph (b)(2)(i) of this section.

(iii) *Agents.* Ensure that any agent to whom it provides this information agrees to implement ~~reasonable~~the administrative, physical, and ~~appropriate security measures to protect the information; and~~technical safeguards in accordance with paragraph (b)(2)(i) of this section.

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

(v) *Contingency plan activation.* Report to the group health plan activation of its contingency plan, adopted in accordance with § 164.308(a)(13) as required by paragraph (b)(2)(i) of this section, without unreasonable delay and in no case later than 24 hours after activation of the contingency plan.

164.316 ~~**Policies and procedures and documentation**~~ Documentation requirements.

(a) *Standard: Documentation.* A covered entity or business associate must~~, in accordance with § 164.306:~~ do all of the following in written form, which may be electronic, taking into consideration the factors in § 164.306(b):

~~(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 or business associate 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~~(1) Document the policies and procedures required to comply with this subpart and how the covered entity or business associate considered the factors at § 164.306(b) in the development of such policies and procedures.

(2) Document each 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~~(b) *Implementation specifications:* —

(~~i~~1) *Time limit ~~(Required).~~.* Retain the documentation required by paragraph (~~b~~)(~~1~~a) 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~~(2) *Availability ~~(Required).~~.* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

~~(iii~~(3) *Updates ~~(Required).~~.* Review and update documentation ~~periodically, and update as needed, in response to environmental or operational changes affecting the~~at least once every 12 months and within a reasonable and appropriate period of time after a security ~~of the electronic protected health information~~measure is modified.