New York State HIPAA Security Matrix
Final HIPAA Security Regulations Published on 2/20/03

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
Security Management Process Implement *policies and procedures* to prevent, detect, contain, and correct security violations.	164.308(a)(1) 	Risk Analysis	(R)	Conduct an accurate and thorough *assessment* of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	**General (pg. 8346):** This standard and its component implementation specifications form the foundation upon which an entity's necessary security activities are built. See NIST SP 800-30, "Risk Management Guide for Information Technology Systems," chapters 3 and 4, January 2002. 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. Some form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards "to ensure compliance . . . by a [covered entity's] officers and employees" could be met without a requirement for a sanction policy. See section 1176(d)(2)(C) of the Act. Accordingly, implementation of these specifications remains mandatory. However, it is important to note that covered entities have the flexibility to implement the standard in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment. **Risk Analysis (pg. 8346-7):** We continue to believe that security measures must remain current, and have added regulatory language in § 164.306(e) as a more precise way of communicating that security measures in general that must be periodically reassessed and updated as needed. The risk analysis implementation specification contains other terms that merit explanation. Under § 164.308(a)(1)(ii)(A), the risk analysis must look at risks to the covered entity's electronic protected health information. 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. All electronic protected health information must be protected at least to the degree provided by these standards. If an entity desires to protect the information to a greater degree than the risk analysis would indicate, it is free to do so. **Sanction Policy (pg. 8347):** Relative to the development of an entity's sanction policy: The sanction policy is a required implementation specification because--(1) the statute requires covered entities to have safeguards to ensure compliance by officers and employees; (2) a negative consequence to noncompliance enhances the likelihood of compliance; and (3) sanction policies are recognized as a usual and necessary component of an adequate security program. 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.
		Risk Management	(R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a).	
		Sanction *Policy*	(R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	
		Information System Activity Review	(R)	Implement *procedures* to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	

 = Policies & Procedures Required  = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
					Information System Activity Review (pg. 8347): 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. The term "internal audit" apparently, based on the comments received, has certain rigid formal connotations we did not intend. We agree that the implementation of formal internal audits could prove burdensome or even unfeasible, to some covered entities due to the cost and effort involved. However, we do not want to overlook the value of internal reviews. Based on our review of the comments and the text to which they refer, it is clear that this requirement should be renamed for clarity and that it should actually be an implementation specification of the security management process rather than an independent standard.
Assigned Security Responsibility	164.308(a)(2)		(R)	Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	**Assigned Security Responsibility (pg. 8347):** In this final rule, we clarify that the final responsibility for a covered entity's security must be assigned to one official. The requirement for documentation is retained, but is made part of § 164.316 below. This policy is consistent with the analogous policy in the Privacy Rule, at 45 CFR 164.530(a), and the same considerations apply. See 65 FR 82744 through 87445. The same person could fill the role for both security and privacy. 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. This decision also aligns this rule with the final Privacy Rule provisions concerning the Privacy Official.
Workforce Security 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.	164.308(a)(3)	Authorization and/or Supervision	(A)	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.	**Authorization and/or Supervision (pg. 8348):** We agree that a "knowledgeable" person may not be available to supervise maintenance personnel. We have accordingly modified this implementation specification so that, in this final rule, we are adopting an addressable implementation specification titled, "Authorization and/or supervision," requiring that workforce members, for example, operations and maintenance personnel, must either be supervised or have authorization when working with electronic protected health information or in locations where it resides (see § 164.308(a)(3)(ii)(A)). Entities can decide on the feasibility of meeting this specification based on their risk analysis. **Workforce Clearance Procedures (pg. 8348):** 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. Effective personnel screening processes may be applied in a way to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis performed by the covered entity. So long as the standard is met and the underlying standard of § 164.306(a) is met, covered entities have choices in how they meet these standards.
		Workforce Clearance Procedure	(A)	Implement *procedures* to determine that the access of a workforce member to electronic protected health information is appropriate.	
		Termination Procedures	(A)	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.	

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
					While we do not believe this requirement should be eliminated, we agree that all the implementation specifications may not be applicable or even appropriate to a given entity. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are not mandatory, but must be addressed. **Termination Procedures (pg. 8348-9):** In this final rule, "Termination procedures" has been made an addressable implementation specification under "Workforce security." 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. ..consideration 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. We further agree with the reasoning of the commenters who asked that these procedures be made optional; therefore, "Termination procedures" is now reflected in this final rule as an addressable implementation specification. We also removed reference to all specific termination activities, for example, changing locks, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others. Policies and procedures implemented to adhere to this standard must be documented (see § 164.316 below). The purpose of termination procedure documentation under this implementation specification is not to detail when or under which circumstances an employee should be terminated. This information would more appropriately be part of the entity's sanction policy. 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 when a termination occurs.
Information Access Management 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.	164.308(a)(4)	Isolating Health Care Clearinghouse Function	(R)	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.	**General (pg. 8358):** 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**.** **Isolating Health Care Clearinghouse (pg. 8349):** Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is minimized. We cannot, however, specifically identify participating parties and access privileges relative to data
		Access Authorization	(A)	Implement *policies and procedures* for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	
		Access Establishment	(A)	Implement *policies and procedures* that, based upon the entity's	

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
		and Modification		access authorization policies, establish, *document*, review, and modify a user's right of access to a workstation, transaction, program, or process.	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 § 164.514(d) in the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information), and is, therefore, being retained. **Access Authorization (pg. 8349):** 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.
Security Awareness and Training Implement a security awareness and training program for all members of its workforce (including management).	106.308(a)(5)	Security Reminders	(A)	Periodic security updates.	**General (pg. 8349-50):** For the standard "Security awareness and training," in § 164.308(a)(5), we require training of the workforce as reasonable and appropriate to carry out their functions in the facility. All proposed training features have been combined as implementation specifications under this standard. Specific implementation specifications relative to content are addressable. The "Virus protection" implementation feature has been renamed "protection from malicious software," because we did not intend by the nomenclature to exclude coverage of malicious acts that might not come within the prior term, such as worms. 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," (broken down into 3 PDF files: Part 1 - document, Part 2 - Appendix A-D, Part 3 - Appendix E) provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities. We also note that covered entities must have discretion in how they implement the requirement, so they can incorporate this training in other existing activities. One approach would be to require this training as part of employee orientation. Security training remains a requirement because of its criticality; however, we have revised the implementation specifications to indicate that the amount and type of training needed will be dependent upon an entity's configuration and security risks. Business associates must be made aware of security policies and procedures, whether through contract language or other means. Covered entities are not required to provide training to business associates or anyone
		Protection from Malicious Software	(A)	*Procedures* for guarding against, detecting, and reporting malicious software.	
		Log-in Monitoring	(A)	*Procedures* for monitoring log-in attempts and reporting discrepancies.	
		Password Management	(A)	*Procedures* for creating, changing, and safeguarding passwords.	

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
					else that is not a member of their workforce. Several commenters objected to the blanket requirement for security awareness training of individuals who may be on site for a limited time period (for example, a single day). Response: Each individual who has access to electronic protected health information must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures. 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). The rule does not contemplate a one-time type of activity as connoted by "orientation," but rather an on-going, evolving process as an entity's security needs and procedures change. Amount and timing of training should be determined by each covered entity; training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information. While initial training must be carried out by the compliance date, we provide flexibility for covered entities to construct training programs. Training can be tailored to job need if the covered entity so desires.
Security Incident Procedures Implement *policies and procedures* to address security incidents.	106.308(a)(6)	Response and Reporting	(R)	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; and *document* security incidents and their outcomes.	**Response and Reporting (pg. 8350-51):** We define a security incident in § 164.304. Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon an entity's environment and the information involved. An entity should be able to rely upon the information gathered in complying with the other security standards, for example, its risk assessment and risk management procedures and the privacy standards, to determine what constitutes a security incident in the context of its business operations. Internal reporting is an inherent part of security incident procedures. This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations. One commenter stated that this requirement should address suspected misuse also. Response: We agree that security incidents include misuse of data; therefore, this requirement is addressed.
Contingency Plan Establish (and implement as needed) *policies and procedures* for responding to an emergency	106.308(a)(7)	Data Backup Plan	(R)	Establish and implement *procedures* to create and maintain retrievable exact copies of electronic protected health information.	**General (pg. 8351):** A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed. Each entity needs to determine its own risk in the event of an emergency that

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.		Disaster Recovery Plan	(R)	Establish (and implement as needed) *procedures* to restore any loss of data.	would result in a loss of operations. A contingency plan may involve highly complex processes in one processing site, or simple manual processes in another. The contents of any given contingency plan will depend upon the nature and configuration of the entity devising it. Without contingency planning, a covered entity has no assurance that its critical data could survive an emergency situation. Recent events, such as September 11, 2001, illustrate the importance of such planning. Contingency planning will be scalable based upon, among other factors, office configuration, and risk assessment. However, in response to the scalability issue raised by the commenter, we have made the testing and revision implementation specification addressable (see § 164.308(a)(7)(ii)). The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low. **Testing and Revision / Applications and Data Criticality (pg. 8351):** Dependent upon the size, configuration, and environment of a given covered entity, the entity should decide if testing and revision of all parts of a contingency plan should be done or if there are more reasonable alternatives. The same is true for the proposed applications and data criticality analysis implementation feature. We have revised the final rule to reflect this approach. **Emergency Mode Operation Plan (pg. 8351):** We have clarified the "Emergency mode operations plan" to show that it only involves those critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.
		Emergency Mode Operation Plan	(R)	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.	
		Testing and Revision Procedure	(A)	Implement *procedures* for periodic testing and revision of contingency plans.	
		Applications and Data Criticality Analysis	(A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	
Evaluation 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 of electronic protected health information, that establishes the	164.308(a)(8)		(R)	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 of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	**Evaluation (pg. 8351-52):** In this final rule, we require covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. 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. 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.

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
extent to which an entity's security policies and procedures meet the requirements of this subpart.					We have revised this section to reflect that evaluation would be both technical and nontechnical components of security. Some commenters asked how certification is possible without specifying the level of risk that is permissible. Response: The level of risk that is permissible is specified by § 164.306(a). How such risk is managed will be determined by a covered entity through its security risk analysis and the risk mitigation activities it implements in order to ensure that the level of security required by § 164.306 is provided.
Business Associate Contracts and Other Arrangement	164.308(b)(1)	*Written Contract or Other Arrangement*	(R)	Business associate contracts and other arrangements. 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. 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. (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; 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.	**General (pg. 8352):** The covered entity must obtain satisfactory assurances from the business associate that it will appropriately safeguard the information in accordance with these standards (see§ 164.314(a)(1)).
				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	

= Policies & Procedures Required = Documentation Required , * See Endnotes

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
				specifications, and requirements of this paragraph and Sec. 164.314(a).	
				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).	

Physical Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
Facility 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.	164.310(a)(1)	Contingency Operations	(A)	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.	**General (pg. 8353):** "Physical safeguards are security measures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." 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. We agree that all implementation specifications may not be appropriate in all situations. While the facility access controls standard must be met, we agree that the implementation specifications should not be required in all circumstances, but should be addressable. In this final rule, all four implementation specifications are addressable. One commenter raised the issue of a potential conflict of authority between those having access to the data and those responsible for checking and maintaining access controls. Response: Any potential conflicts should be identified, addressed, and resolved in the policies and procedures developed according to the standards under § 164.308. **Facility Security Plan (pg. 8353):** The facility security plan is an addressable implementation specification. However, the 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.
		Facility Security Plan	(A)	Implement *policies and procedures* to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	
		Access Control and Validation Procedures	(A)	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.	
		Maintenance Records	(A)	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).	
Workstation Use	164.310(b)		(R)	Implement *policies and procedures* that specify the proper functions to be performed, 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.	**General (pg. 8354):** For clarity, we have added the definition of "workstation" to § 164.304 and deleted the word "terminal" from the description of workstation use in § 164.310(b).
Workstation Security	164.310(c)		(R)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	**General (pg. 8354):** We agree that what constitutes an appropriate solution to a covered entity's workstation security issues is dependent on the entity's risk analysis and risk management process. Because many commenters incorrectly interpreted the examples as the required and only solution for securing the workstation location, we have modified the regulations text description to generalize the requirement (see § 164.310(c)). Also, for clarity, the title "Secure workstation location" has been changed to "Workstation security" (see also the definition of "Workstation" at § 164.304).
Device and Media Controls	164.310(d)(1)	Disposal	(R)	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.	**General (pg. 8354):** The media examples used were not intended to represent all possible physical types of hardware and/or software. Removable media devices, although not specifically listed, are not intended to be excluded.

= Policies & Procedures Required = Documentation Required , * See Endnotes

Implement *policies and procedures* that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.		Media Re-use	(R)	Implement *procedures* for removal of electronic protected health information from electronic media before the media are made available for re-use.	The term "facility" refers to the physical premises and the interior and exterior of a building(s). We have added this definition to § 164.304. While the "Device and media controls" standard must be met, we believe, based upon further review, that implementation of all specifications would not be necessary in every situation, and might even be counter-productive in some situations. For example, small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large health care providers or health plans. We have, therefore, reclassified the "Accountability and data backup" implementation specification as addressable to provide more flexibility in meeting the standard. **Accountability (pg. 8354):** This implementation specification does not address audit trails within systems and/or software. Rather it requires a record of the actions of a person relative to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. For example, the appropriate mechanism for a given entity may be manual, such as receipt and removal restricted to specific persons, with logs kept. Maintaining accountability in such a fashion should have a minimal, if any, effect on system resources and services. **Backup (pg. 8354):** The data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business "as usual" in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.
		Accountability	(A)	*Maintain a record* of the movements of hardware and electronic media and any person responsible therefore.	
		Data Backup and Storage	(A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	

Technical Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
Access Control Implement technical *policies and procedures* 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).	164.312(a)(1)	Unique User Identification	(R)	Assign a unique name and/or number for identifying and tracking user identity.	**Access Control (pg. 8355):** 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. Proposed implementation features titled "Context-based access," "Role-based access," and "User-based access" have been deleted and the access control standard at § 164.312(a)(1) states the general requirement. **Automatic Logoff (pg. 8355):** This final rule has been written to clarify that the proposed implementation feature of automatic logoff now appears as an addressable access control implementation specification and also permits the use of an equivalent measure. **Encryption (pg. 8355):** 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. **Emergency Access Procedure (pg. 8355):** 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 man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.
		Emergency Access Procedure	(R)	Establish (and implement as needed) *procedures* for obtaining necessary electronic protected health information during an emergency.	
		Automatic Logoff	(A)	Implement *electronic procedures* that terminate an electronic session after a predetermined time of inactivity.	
		Encryption and Decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.	
Audit Controls	164.312(b)		(R)	Implement hardware, software, and/or *procedural mechanisms* that record and examine activity in information systems that contain or use electronic protected health information.	**General (pg. 8355):** We support the use of a risk assessment and risk analysis to determine how intensive any audit control function should be. We believe that the audit control requirement should remain mandatory, however, since it provides a means to assess activities regarding the electronic protected health information in an entity's care. **Audit Controls (pg. 8355-6):** We believe that it is appropriate to specify audit controls as a type of technical safeguard. 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 It should be noted that although the Privacy Rule does not incorporate a requirement for an

= Policies & Procedures Required = Documentation Required , * See Endnotes

Technical Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
					"audit trail" function, it does call for providing an accounting of certain disclosures of protected health information to an individual upon request. 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).
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	**General (pg. 8356):** We adopt the suggested "integrity" terminology because it more clearly describes the intent of the standard. We retain the meaning of the term "Data authentication" under the addressable implementation specification "Mechanism to authenticate data," and provide an example of a potential means to achieve data integrity. 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 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.
Person or Entity Authentication Implement *procedures* to verify that a person or entity seeking access to electronic protected health information is the one claimed.	164.312(d)		(R)		**General (pg. 8356):** We agree with the commenters that many different mechanisms may be used to authenticate entities, and this final rule now reflects this fact by not incorporating a list of implementation specifications, in order to allow covered entities to use whatever is reasonable and appropriate. "Digital signatures" and "soft tokens" may be used, as well as many other mechanisms, to implement this standard.
Transmission Security Implement technical security measures to guard against unauthorized access to electronic protected health information that is being	164.312(e)(1)	Integrity Controls	(A)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	**General (pg. 8356-7):** This final rule has been significantly revised to reflect a much simpler and more direct requirement. The term "Communications/network controls" has been replaced with "Transmission security" to better reflect the requirement that, when electronic protected health information is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk. We agree with the commenters that switched, point-to-point connections, for example, dial-

= Policies & Procedures Required = Documentation Required , * See Endnotes

Technical Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
transmitted over an electronic communications network.					up lines, have a very small probability of interception. Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet. As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption. We do not use the term "open network" in this final rule because its meaning is too broad. We include as an addressable implementation specification the requirement that transmissions be encrypted when appropriate based on the entity's risk analysis. Three commenters asked for clarification and guidance regarding 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. Commenters asked for guidance as to what was their obligation to protect data received in this manner. Response: The manner in which electronic protected health information is received by a covered entity does not affect the requirement that security protection must subsequently be afforded to that information by the covered entity once that information is in possession of the covered entity.

Technical Safeguards

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	

Organizational Requirements

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
Business associate contracts or other arrangements.	164.314(a)(1)			(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.	**Organizational Requirements (pg. 8358)**: In this final rule, we have adopted the concepts of hybrid and affiliated entities, as previously defined in § 164.504, and now defined in § 164.103, and business associates as defined in § 160.103, to be consistent with the Privacy Rule. General organizational requirements related to affiliated covered entities and hybrid entities are now contained in a new § 164.105. The proposed chain of trust partner agreement has been replaced by the standards for business associate contracts or other arrangements and the standards for group health plans. Consistent with the statute and the policy of the Privacy Rule, this final rule does not require noncovered entities to comply with the security standards. Since the security standards are intended to support the protection of electronic information protected by the Privacy Rule, it makes sense to incorporate organizational requirements that parallel those required of covered entities by the Privacy Rule. This policy will also minimize the burden of complying with both rules. The "larger organization" is the overall business entity that a clearinghouse would be part of. Under the Security Rule, the larger organization must assure that the health care clearinghouse function has instituted measures to ensure only that electronic protected health information that it processes is not improperly accessed by unauthorized persons or other entities, including the larger organization. Internal electronic communication within the larger organization will not be covered by the rule if it does not involve the clearinghouse, assuming that it has designated health care components, of which the health care clearinghouse is one. External communication must be protected as sent by the clearinghouse, but need not be protected once received.
				(ii) 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.	
		Business associate contracts	(R)	(i) The *contract* between a covered entity and a business associate must provide that the business associate will-- (A) 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) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) 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.	

= Policies & Procedures Required = Documentation Required , * See Endnotes

Organizational Requirements

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
		Other arrangements	(R)	(ii) (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	

Organizational Requirements

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable *		Implementation Standards	Preamble Notes **
Requirements for group health plans	164.314(b)(1)			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.	
	164.314(b)(2)	The plan *documents* of the group health plan must be amended to incorporate provisions to require the plan sponsor to--	(R)	(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.	

Policies and Procedures and Documentation Requirements

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

Standards	164.316(a)	Implementation Specifications (R) = Required (A) = Addressable *			
Policies and Procedures	164.312(b)(1) 			(a) 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.	
Documentation	164.312(b)(2)(i) 			(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.	
	164.312(b)(2)(ii)	Time Limit	(R)	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.	
	164.312(b)(2)(iii)	Availability	(R)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	
	164.312(b)(2)(iii)	Updates	(R)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	

 = Policies & Procedures Required  = Documentation Required , * See Endnotes

Endnotes:

*** Required/Addressable Requirements:** In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following:

(a) implement one or more of the addressable implementation specifications;
(b) implement one or more alternative security measures;
(c) implement a combination of both; or
(d) not implement either an addressable implementation specification or an alternative security measure. In all cases, the covered entity must meet the standards, as explained below.

The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. Based upon this decision the following applies:

(a) If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.

(b) If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity, but the standard cannot be met without implementation of an additional security safeguard, the covered entity may implement an alternate measure that accomplishes the same end as the addressable implementation specification. An entity that meets a given standard through alternative measures must document the decision not to implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312 (c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might well be more practical and afford a sufficient safeguard to make paper copies of the data.

(c) A covered entity may also decide that a given implementation specification is simply not applicable (that is, neither reasonable nor appropriate) to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met. For example, under the information access management standard, an access establishment and modification implementation specification reads: "implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

**** Preamble Notes**: Information in this column references excerpts from the Preamble to the final HIPAA Administrative Simplification Security Rule published on 2/20/03. The excerpts selected are those which might provide guidance or additional information to assist with the implementation of HIPAA. Note: Interpretive comments by federal agencies such as those found in the preamble sections of regulations are not formally part of the regulations, do not have "the force of law" and thus are not, technically, legally binding.