

Healthcare Lockdown—Getting Ready for HIPAA Security by James H. Barclay

Page 22

Recent federal HIPAA privacy rules are the most significant event in healthcare since Medicare and Medicaid because they affect so many healthcare providers and patients. Their vast coverage extends well beyond their intended “covered entities”—health plans, clearinghouses, healthcare providers (and their untold millions of patients with “new” patient rights)—and reaches companies, so called “business associates,” who work for covered entities. Many unsuspecting employers, including some law firms, were also caught up by the sweep of the rules.

During 2003, lawyers nationwide put finishing touches on policies and procedures as they helped countless covered entity clients meet HIPAA privacy compliance deadlines. Now another major HIPAA compliance deadline looms on the horizon: April 20, 2005—but this time, it’s HIPAA security. The HIPAA security rules are just as sweeping as HIPAA privacy and affect the same covered entities, their patients, and others. For these reasons and because so many tasks required by the rules are uniquely within the purview of counsel, such as developing and implementing HIPAA security compliance plans, with their necessary policies and procedures—and then monitoring them for effectiveness—HIPAA security presents a significant opportunity for counsel to provide value added services to covered entity clients, especially during the scant few months before April 20, 2005.

This article discusses the basic HIPAA security concepts, standards, and implementation specifications in the HIPAA security rules,¹ points out some significant opportunities for counsel, and offers some practical suggestions for HIPAA security compliance efforts.

HIPAA Security Concepts—Getting a Handle on the HIPAA Security Rules

A covered entity² must comply with HIPAA security rule standards, implementation specifications, and other requirements³ when electronic protected health information (“ePHI”) is involved. The accompanying “at a glance” information (see page 30) provides some basic HIPAA security concepts. Generally, HIPAA security requires a covered entity to ensure the confidentiality,⁴ integrity,⁵ and availability⁶ of all ePHI the covered entity creates, receives, maintains, or transmits⁷; protect against any reasonably anticipated threats or hazards to the security or integrity of such information⁸; protect against any reasonably anticipated uses or disclosures of such information⁹ not permitted or required under the HIPAA privacy rules¹⁰; and ensure compliance with the HIPAA security rules by its workforce.¹¹

Rules Designed to be Scalable and Flexible

The HIPAA security rules permit a covered entity to use any security measure that allows reasonable and appropriate implementation of its standards and implementation specifications.¹² However, in deciding which security measures to use, the following factors about the covered entity must be taken into consideration when making that decision: its size, complexity, and capabilities; its technical infrastructure, hardware and software security capabilities; costs; and the probability and criticality of potential risks to ePHI.¹³ Counsel are cautioned that although the rules explicitly state that these factors are to be taken into consideration when implementing policies and procedures, the standard requiring policies and procedures is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other HIPAA security rule requirement.¹⁴

How Rules Are Organized and Presented

HIPAA security rules proceed from broad principles that are narrowed by standards and further refined by implementation specifications. At the highest level, they are comprehensive and address all aspects of security. They are scalable and flexible, and thus can be tailored for the particular circumstances of each covered entity, and are technology-neutral because they favor no specific technology. The rules establish standards for administrative,¹⁵ physical,¹⁶ technical¹⁷ “safeguards” and “requirements” addressing organizational matters,¹⁸ and policies, procedures, and documentation.¹⁹ Most standards have “implementation specifications”—more detailed compliance actions—some of which are mandatory while others are “addressable.” Implementation specifications are specific ways to implement HIPAA standards and are a prominent feature of the HIPAA security rules. Most implementation specifications are required and therefore must be implemented.²⁰ However, some specifications are “addressable” and may be implemented as reasonable and necessary. HIPAA security safeguards and standards, together with required and addressable implementation specifications, are in the following table:²¹

- **Four-step Process to Document Whether to Implement Addressable Implementation Specification**

If an addressable specification is not reasonable or is not appropriate, a covered entity must go through a four-step process in order to do one of two things: document either implementation of an equivalent measure or document that the measure is not applicable to the organization.²³ This evaluation process, and its resulting documentation, are key functions for counsel. For each addressable specification, a covered entity must assess whether the specification is a reasonable and appropriate safeguard in its environment when analyzed with reference to the safeguard’s likely contribution to protecting the entity’s ePHI. Then, as applicable to the covered entity, it must either implement the implementation specification or document why it would not be reasonable and appropriate, and, if reasonable, implement an equivalent alternative measure.²⁴

- **Documentation Maintenance, Updates Present Unique Opportunities**

The documentation maintenance requirements of the HIPAA security rules present another significant opportunity to counsel for covered entities. Counsel should be mindful that the rules require *as-needed* review and modification of security measures so that reasonable and appropriate protection of ePHI are continuously provided.²⁵ Covered entities are also required to periodically review and update documentation, including policies and procedures, when circumstances affecting the security of ePHI change.²⁶ Counsel should be alert to ensure that covered entities comply with these important maintenance and updating requirements.

- **Administrative Safeguards**

The HIPAA security rules require covered entities to develop and implement policies and procedures addressing primary areas of emphasis, called “safeguards.” Safeguards, together with their accompanying implementation specifications, must be implemented. Administrative safeguards²⁷ are administrative activities to manage the selection, development, implementation, and maintenance of security measures²⁸ to protect ePHI and to manage the workforce in relation to protecting ePHI.²⁹ They consist of policies, procedures, and administrative actions for maintaining security measures and managing the workforce.³⁰

- **HIPAA Security Management Standard Focuses on Security Violations**

The security management standard is designed to ensure prevention, detection, containment, and correction of security violations.³¹ Security management begins with a risk analysis and assessment, requires sanctions, and necessarily involves ongoing reviews. The security management standard has an internal tension because it requires policies and procedures to ensure appropriate access³² to ePHI on the one hand while preventing inappropriate access on the other hand.³³ It has implementation specifications that include risk analysis, risk management, sanctions, and information system activity review.³⁴

The implementation specification governing risk analysis calls for covered entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality,

integrity, and availability of ePHI.³⁵ The risk management implementation specification requires measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.³⁶ The implementation specification involving sanctions mandates appropriate sanctions against workforce members who fail to comply with the covered entity's security policies and procedures.³⁷ Information system activity review is an implementation specification of the security management standard. Under the rules, an information system is defined as an interconnected set of information resources under direct management and control that shares common functionality.³⁸ A "system" commonly includes hardware, software, information, data, applications, communications, and people. The rules require information system activity reviews through procedures such as audit logs, access reports, and security incident³⁹ tracking reports.⁴⁰ Under the rule, regular reviews of information system records are required.⁴¹ This effort requires appropriate policies and procedures and implicates the technology needed to create audit logs, access reports, and incident tracking reports.

- **Designate Security Officer to Comply With Assigned Security Responsibility Standard**
Under the standard for assigning security responsibility, a covered entity must designate a security official responsible for developing and implementing HIPAA security policies and procedures for the covered entity.⁴² The security official can be a member of the workforce. Although HIPAA privacy officers are prime candidates for the position of security official, counsel for the covered entity can certainly perform each of these functions.

- **Workforce Security Standard Addresses Getting, Limiting Access**
The workforce standard requires policies and procedures to ensure appropriate access to ePHI by all members of the covered entity's workforce while preventing inappropriate access at the same time.⁴³ This standard has specifications requiring procedures for authorization or supervision of workforce members who work with ePHI or who work in locations where ePHI might be accessed; procedures to determine that access of a workforce member to ePHI is appropriate; and policies and procedures for terminating access to ePHI when employment ends or if access by a workforce member to ePHI is inappropriate.⁴⁴

- **Information Access Management Standard**
The information access management standard requires policies and procedures authorizing access to ePHI consistent with the HIPAA privacy rules at 45 CFR §164.500 *et seq.*⁴⁵ This rule implicates the "minimum necessary" provisions of the HIPAA privacy rule⁴⁶ under which covered entities are required to limit PHI to the minimum necessary to accomplish the intended purpose of the intended use or disclosure.

Clearinghouse functions⁴⁷ of a covered entity, if any, must be isolated—"firewalled," for example—from the remainder of the organization.⁴⁸ Two implementation specifications must also be considered in the context of this standard: access authorization⁴⁹ and access establishment and modification.⁵⁰ Simply stated, access authorization involves developing and implementing criteria to control access to ePHI through workstations,⁵¹ transactions, programs, processes, or any other mechanism.⁵² These criteria should identify personnel needing access and what PHI is accessible. Access criteria can be user-based,⁵³ role-based, or context-based. Once authorization is established and documented, the process of actually accessing ePHI should be documented, for example, areas to which access is granted; usable equipment; permitted applications; accessible types of data; and function limitations, if any.

Counsel should develop policies and procedures requiring that personnel who authorize access should also review and approve access authorizations. Counsel should also be mindful that the documents used for access authorization may also form an explicit agreement whereby understanding of applicable policies and procedures is acknowledged, training is confirmed, rules of conduct are set forth, sanctions for violations are set forth, and other employment-related issues may be addressed.

Policies and procedures addressing access modification should state circumstances under which rights to access workstations, terminals, processes, applications, etc., will be modified.⁵⁴ These particular policies and procedures can be particularly sensitive under circumstances involving

layoffs, terminations, and other situations where a workforce member's interests may be adverse to the covered entity.

- Security Awareness and Training Standard

Unless the workforce is made aware of, trained, and reminded about the covered entity's security policies and procedures, the best drafting efforts of counsel will be for naught. Standards for HIPAA security awareness and training requirements⁵⁵ are similar to training requirements for HIPAA privacy⁵⁶ in terms of general training about policies and procedures. Like the HIPAA privacy rules, the security rules require awareness and training for all members of the workforce, including management.⁵⁷

The implementation specifications involving security awareness and training require periodic updates,⁵⁸ another area in which counsel should schedule and participate; procedures for guarding against, detecting, and reporting malicious software;⁵⁹ procedures for monitoring log-in attempts and reporting discrepancies;⁶⁰ and procedures for creating, changing, and safeguarding passwords⁶¹ (confidential authentication information composed of a string of characters⁶²).

- Security Incident Procedures Standard

Under the security incident standard, covered entities are required to implement policies and procedures to address security incidents⁶³—*unauthorized* access, use, disclosure, modification, or destruction of information or interference with system operations, successful or otherwise.⁶⁴ The incident procedure standard has a single implementation specification with three separate parts: identify and respond to suspected or known security incidents; mitigate harmful effects of security incidents; and document incidents and outcomes.⁶⁵

- HIPAA Contingency Plan Standard Requires Plans for Emergencies or Events that Affect ePHI

The contingency plan standard requires covered entities to establish and implement policies and procedures for responding to emergencies and other circumstances that affect ePHI such as fire, vandalism, system failure, and any natural disaster that damages systems containing ePHI.⁶⁶ The contingency planning rule has three required and two implementation specifications. A data backup plan, a disaster recovery plan, and an emergency mode plan are required.⁶⁷ Testing and revisions procedures, as well as applications and data criticality analysis, are addressable.⁶⁸ The data backup plan must have procedures to ensure that the covered entity creates and maintains retrievable exact copies of ePHI.⁶⁹ Counsel in Florida are accustomed to natural disasters such as hurricanes but other circumstances such as extensive forest fires can create situations where disaster recovery plans must be implemented. When disasters occur, covered entities may not be able to perform critical functions for extended periods of time. Disaster recovery plans must have procedures to restore any loss of data.⁷⁰ Covered entities must establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.⁷¹ An addressable implementation specification requires procedures for periodic testing and revision of contingency plans.⁷² Also addressable is the applications and data criticality analysis implementation specification.⁷³ This effort involves assessing applications (software and other means of processing information) used to perform work and the impact (criticality) on the organization if one or all of the applications using ePHI were lost or compromised. In other words, the relative criticality of specific applications and data in support of other contingency plan components must be assessed. The process identifies potential ways applications might fail and predicts the consequences. The more critical an application, the higher priority an application will have during restoration and recovery.

- Covered Entities Required to Evaluate Policies and Procedures

The important evaluation standard requires periodic technical and nontechnical evaluations of how the covered entity's policies and procedures meet the requirements of the HIPAA security rule. The initial evaluation is to be based on the HIPAA security standards. Subsequent evaluations are to be conducted in response to environmental or operational changes that affect security of ePHI.⁷⁴ This is yet another area that can be scheduled, managed, and implemented by counsel for the covered entity.

- HIPAA Security Physical Safeguards

Physical safeguards are physical measures, plus policies and procedures, to protect a covered entity's electronic information systems and related building and equipment from natural and environmental hazards and unauthorized intrusion.⁷⁵ The second of three major safeguards, its competing goals require a covered entity to implement policies and procedures to limit physical access to its electronic information systems, and the facility⁷⁶ or facilities where housed on the one hand, while ensuring that only properly authorized access is allowed on the other hand.⁷⁷ Physical safeguards prevent unauthorized access and involve workstations, computers, disasters and hazards, equipment, rooms, and buildings.⁷⁸

- Facility Access Controls Standard

The facility access controls standard has four implementation specifications. The one for contingency operations requires procedures that allow facility access in support of restoration of lost data under a disaster recovery plan. It also requires an emergency mode operation plan.⁷⁹ The facility security plan implementation specification requires policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering, and theft.⁸⁰ The implementation specification for access control and validation procedures requires procedures to control and validate access to facilities, including visitors, based on their role or function.⁸¹ It also covers control of access to software programs for testing and revision.⁸² The implementation specification for maintenance records requires policies and procedures to document repairs and modifications to physical components of a facility related to security such as hardware, walls, doors, and locks.⁸³

- Workstation Use and Security Standards

Separate standards govern use and security of workstations. The workstation use standard requires policies and procedures specifying proper functions to be performed on workstations, the manner in which those functions are to be performed, and the physical attributes surrounding specific workstations or class of workstations that can access ePHI.⁸⁴ The workstation security standard requires physical safeguards for all workstations that access ePHI in order to confine and restrict access to authorized users.⁸⁵

- Device and Media Controls Standard

This standard requires policies and procedures governing not only receipt and removal of hardware and electronic media that contain ePHI into and out of the facility but also the movement of these items within the facility.⁸⁶ The implementation specification dealing with device and media disposal requires policies and procedures to address final disposition of ePHI and the hardware or electronic media on which it is stored.⁸⁷ Under the implementation specification for media re-use, a covered entity must have procedures for removal of ePHI from electronic media before the media are made available for re-use.⁸⁸ Implementation specifications require maintaining a record of the movements of hardware and electronic media and any person responsible for them⁸⁹ and creation of data backup and storage by requiring creation of a retrievable exact copy of ePHI when needed but before equipment is moved.⁹⁰

- HIPAA Technical Safeguards

Technical safeguards,⁹¹ the third major HIPAA safeguard, are together the technology and the policy and procedures for its use that protect and control access to ePHI.⁹²

- Access Control Standard

This standard requires policies and procedures for electronic information systems that maintain ePHI so that access is allowed only to those persons or software programs that have been granted appropriate access rights.⁹³ Implementation specifications for access control deal with unique user identification, emergency access procedures, automatic log-off, encryption,⁹⁴ and decryption. To comply with implementation specifications, a covered entity must assign a unique name and/or number to identify and track user identity⁹⁵ and establish and implement procedures

for obtaining necessary ePHI during an emergency.⁹⁶ Implementation specifications also involve procedures to terminate an electronic session after a predetermined time of inactivity⁹⁷ and implementation of a mechanism to encrypt and decrypt ePHI.⁹⁸

- **Audit Controls, Integrity, Authentication, and Transmission Security Standards**

The audit controls standard requires implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.⁹⁹ The integrity standard requires implementation of policies and procedures to protect ePHI from improper alteration or destruction.¹⁰⁰ To authenticate¹⁰¹ electronic PHI, the implementation specification requires implementation of electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.¹⁰² The “person or entity authentication” standard requires procedures to verify that a person or entity seeking access to ePHI information is the one claimed.¹⁰³ The transmission standard requires implementation of measures to guard against unauthorized access to ePHI transmitted over an electronic communications network.¹⁰⁴ The implementation specifications for integrity controls require measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of¹⁰⁵ and a mechanism to encrypt ePHI as appropriate.¹⁰⁶

- **Standards, Requirements for Business Associate Contracts and Other Arrangements**

A covered entity may permit a business associate¹⁰⁷ to create, receive, maintain, or transmit ePHI on the covered entity’s behalf but only if the covered entity receives certain “satisfactory assurances” that the business associate will appropriately safeguard the information.¹⁰⁸ Unless exempt,¹⁰⁹ satisfactory assurances must be documented by a written agreement, or other arrangement that meets applicable requirements such as a memorandum of law or governing laws with requirements that satisfy HIPAA security requirements. Although the security rule requires business associate agreements when business associates are utilized,¹¹⁰ the minimum requirements of the contract (or other arrangement) between a covered entity and its business associate will depend on whether both are governmental entities. The rules set out the required terms and conditions¹¹¹ when both are governmental entities.¹¹²

Required terms and conditions for all other business associate agreements include the following:

- 1) Implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI it creates, receives, maintains, or transmits on behalf of the covered entity as required by the HIPAA privacy rules;¹¹³
- 2) Ensure that any agent, including a subcontractor, to whom it provides ePHI likewise agrees to implement reasonable and appropriate safeguards to protect it;¹¹⁴
- 3) Report to the covered entity any security incident to the covered entity;¹¹⁵ and
- 4) Authorize termination¹¹⁶ of the business associate agreement by the covered entity if the business associate violates a material term of the agreement.¹¹⁷

- **Standards for HIPAA Security Policies and Procedures**

HIPAA security policies and procedures are not optional; they are mandatory.¹¹⁸ As noted earlier, a covered entity may use any security measure that allows it to reasonably and appropriately implement the HIPAA standards and implementation specifications.¹¹⁹ In deciding which security measures to use, four factors must be taken into consideration: size, complexity, and capabilities; technical infrastructure, hardware and software security capabilities; costs; and probability and criticality of risks to ePHI.¹²⁰ Although these factors are to be taken into consideration, the HIPAA security policy and procedure rule¹²¹ is not to be construed to permit or excuse an action that violates any other standard, implementation specification or other HIPAA security rule requirement. Tactically, HIPAA security policies and procedures must guide the workforce. Strategically, they may serve an important evidentiary role in demonstrating the organization’s commitment and good faith compliance efforts.

- **HIPAA Security Standard for Documentation Addresses Retention and Updates**

Documentation of HIPAA security policies and procedures is another area in which counsel can

provide added value to covered entities. For example, the documentation standard requires a covered entity to maintain the policies and procedures that will be implemented to comply with the HIPAA security rule in written (which may be electronic) form.¹²² If an action, activity, or assessment is required to be documented, a covered entity must maintain a written (or electronic) record of the action, activity, or assessment.¹²³ In terms of formulating a retention policy for HIPAA security purposes, policies, and procedures must be retained, in either electronic or written format, six years from the date created or last in effect, whichever is later.¹²⁴ In addition to retention requirements, documentation is to be made available to those responsible for implementing the policies and procedures.¹²⁵ Adding further to the potential added value of proactive counsel is the implementation specification that mandates periodic documentation reviews, and updates as needed, in response to environmental operational changes affecting the security of ePHI.¹²⁶ Compliance by a covered entity with this requirement is virtually certain to involve legal counsel.

Conclusion

HIPAA security rules are pervasive in terms of their impact and effect because they govern so many covered entities and their patients. Moving forward with HIPAA security compliance provides a unique opportunity for counsel to provide added value in addition to services customarily rendered on behalf of covered entities. By preparing policies and procedures in advance of the April 20, 2005, HIPAA security compliance date, and then monitoring covered entity compliance, counsel can provide invaluable assistance and advice to covered entity clients.

¹ Rules implementing the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) are found in 45 C.F.R. subch. C. The HIPAA security rules discussed in this article are found in 45 C.F.R. §164.302 *et seq.*

² 45 C.F.R. §160.103.

³ 45 C.F.R. §164.302.

⁴ *Confidentiality*, as defined in 45 C.F.R. §164.304, is when data or information is not made available or disclosed to unauthorized persons or processes.

⁵ Integrity means data or information that have not been altered or destroyed in an unauthorized manner. See 45 C.F.R. §164.304.

⁶ Under 45 C.F.R. §164.304, availability means data or information is accessible and usable upon demand by an authorized person.

⁷ 45 C.F.R. §164.306(a)(1).

⁸ 45 C.F.R. §164.306(a)(2).

⁹ 45 C.F.R. §164.306(a)(3).

¹⁰ 45 C.F.R. §164.500 *et seq.*

¹¹ 45 C.F.R. §164.306(a)(4).

¹² 45 C.F.R. §164.306(b)(1).

¹³ 45 C.F.R. §164.306(b)(2)(i)–(iv).

¹⁴ 45 C.F.R. §164.316(a).

¹⁵ 45 C.F.R. §164.308.

¹⁶ 45 C.F.R. §164.310.

¹⁷ 45 C.F.R. §164.312.

¹⁸ 45 C.F.R. §164.314.

¹⁹ 45 C.F.R. §164.316 .

²⁰ 45 C.F.R. §164.306(d)(1).

²¹ A matrix in C.F.R. Part 164, subch. C, Appendix A contains a similar but less extensive list.

²² The HIPAA rules do not explicitly cast “policies and procedures and documentation” as HIPAA security “safeguards,” but only as “requirements.” Because they actually can and do function as safeguards, they have been categorized that way in this table.

²³ 45 C.F.R. §164.306(d)(3).

²⁴ 45 C.F.R. §164.306(d)(3)(A)–(B).

²⁵ 45 C.F.R. §164.306(e).

²⁶ 45 C.F.R. §164.316(b)(2)(iii).

²⁷ *Administrative safeguards* are administrative activities (actions, policies, procedures) to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the workforce in relation to protection of that information. See 45 C.F.R. §164.304.

²⁸ *Security measures* are all of the administrative, physical, and technical safeguards in an information system. See 45 C.F.R. §164.304.

²⁹ 45 C.F.R. §164.304.

³⁰ 45 C.F.R. §164.308.

³¹ 45 C.F.R. §164.308(a)(1)(i).

³² *Access* is defined in 45 C.F.R. §164.304 as the ability to read, write, modify, or communicate data, communicate data or information, or otherwise use any system resource. The definition does not, however, apply to the term as used in the HIPAA privacy rules.

³³ 45 C.F.R. §164.308(a)(3)(i).

³⁴ 45 C.F.R. §164.308(a)(1)(ii)(A)–(D).

³⁵ 45 C.F.R. §164.308(a)(1)(ii)(A).

³⁶ 45 C.F.R. §164.308(a)(1)(ii)(B).

³⁷ 45 C.F.R. §164.308(a)(1)(ii)(C).

³⁸ 45 C.F.R. §164.304.

³⁹ Under 45 C.F.R. §164.304, a *security incident* is an attempted, or successful, unauthorized access, use, disclosure, modification, or destruction of information. The term also includes interference with system operations in an information system.

⁴⁰ 45 C.F.R. §164.308(a)(1)(ii)(D).

⁴¹ 45 C.F.R. §164.308(a)(1)(ii)(D).

⁴² 45 C.F.R. §164.308(a)(2).

⁴³ 45 C.F.R. §164.308(a)(3)(i).

⁴⁴ 45 C.F.R. §164.308(a)(3)(ii)(A)–(C).

⁴⁵ 45 C.F.R. §164.308(a)(4)(i).

⁴⁶ 45 C.F.R. §164.502(b).

⁴⁷ *Healthcare clearinghouse*, as defined in 45 C.F.R. §160.103, means a public or private entity, including a billing service, repricing company, community health management information system, or community health information system, and “value-added” networks and switches, that does either of the following functions: 1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; 2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

⁴⁸ 45 C.F.R. §164.308(a)(4)(ii)(A).

⁴⁹ 45 C.F.R. §164.308(a)(4)(ii)(B).

⁵⁰ 45 C.F.R. §164.308(a)(4)(ii)(C).

⁵¹ *Workstation* is defined in 45 C.F.R. 164.304 as an electronic computing device (laptop or desktop computer, for example) or any other device that performs similar functions. The term includes electronic media stored in its immediate environment.

⁵² 45 C.F.R. §164.308(a)(4)(ii)(B).

⁵³ 45 C.F.R. §164.304 defines *user* as a person or entity with authorized access.

⁵⁴ 45 C.F.R. §164.308(a)(4)(ii)(C).

⁵⁵ 45 C.F.R. §164.308(a)(5).

⁵⁶ 45 C.F.R. §164.530(b).

⁵⁷ 45 C.F.R. §164.308(a)(5)(i).

⁵⁸ 45 C.F.R. §164.308(a)(5)(ii)(A).

⁵⁹ 45 C.F.R. §164.308(a)(5)(ii)(B). *Malicious software* is defined at 45 C.F.R. §164.304 as software (viruses, for example) designed to damage or disrupt a system.

⁶⁰ 45 C.F.R. §164.308(a)(5)(ii)(C).

⁶¹ 45 C.F.R. §164.308(a)(5)(ii)(D).

⁶² 45 C.F.R. §164.304.

⁶³ 45 C.F.R. §164.308(a)(6).

⁶⁴ 45 C.F.R. §164.304.

⁶⁵ 45 C.F.R. §164.308(a)(6)(ii).
⁶⁶ 45 C.F.R. §164.308(a)(7)(i).
⁶⁷ 45 C.F.R. §164.308(a)(7)(ii)(A)(C).
⁶⁸ 45 C.F.R. §164.308(a)(7)(ii).
⁶⁹ 45 C.F.R. §164.308(a)(7)(ii)(A).
⁷⁰ 45 C.F.R. §164.308(a)(7)(ii)(B).
⁷¹ 45 C.F.R. §164.308(a)(7)(ii)(C).
⁷² 45 C.F.R. §164.308(a)(7)(ii)(D).
⁷³ 45 C.F.R. §164.308(a)(7)(ii)(E).
⁷⁴ 45 C.F.R. §164.308(a)(8).
⁷⁵ 45 C.F.R. §164.304.
⁷⁶ Under 45 C.F.R. §164.304, *facility* is defined to include not only the physical premises but also the interior and exterior of a building or buildings.
⁷⁷ 45 C.F.R. §164.310(a)(1).
⁷⁸ 45 C.F.R. §164.310.
⁷⁹ 45 C.F.R. §164.310(a)(2)(i).
⁸⁰ 45 C.F.R. §164.310(a)(2)(ii).
⁸¹ 45 C.F.R. §164.310(a)(2)(iii).
⁸² *Id.*
⁸³ 45 C.F.R. §164.310(a)(2)(iv).
⁸⁴ 45 C.F.R. §164.310(b).
⁸⁵ 45 C.F.R. §164.310(c).
⁸⁶ 45 C.F.R. §164.310(d)(1).
⁸⁷ 45 C.F.R. §164.310(d)(2)(i).
⁸⁸ 45 C.F.R. §164.310(d)(2)(ii).
⁸⁹ 45 C.F.R. §164.310(d)(2)(iii).
⁹⁰ 45 C.F.R. §164.310(d)(2)(iv).
⁹¹ 45 C.F.R. §164.304.
⁹² 45 C.F.R. §164.312.
⁹³ 45 C.F.R. §164.312(a)(1).
⁹⁴ *Encryption* is defined at 45 C.F.R. §164.304 as use of an algorithmic process to transform data into a form where there is a low probability of assigning meaning without use of a confidential process or key.
⁹⁵ 45 C.F.R. §164.312(a)(2)(i).
⁹⁶ 45 C.F.R. §164.312(a)(2)(ii).
⁹⁷ 45 C.F.R. §164.312(a)(2)(iii).
⁹⁸ 45 C.F.R. §164.312(a)(2)(iv).
⁹⁹ 45 C.F.R. §164.312(b).
¹⁰⁰ 45 C.F.R. §164.312(c)(1).
¹⁰¹ Under 45 C.F.R. §165.304, *authentication* means corroboration that a person is the one claimed.
¹⁰² 45 C.F.R. §164.312(c)(2).
¹⁰³ 45 C.F.R. §164.312(d).
¹⁰⁴ 45 C.F.R. §164.312(e).
¹⁰⁵ 45 C.F.R. §164.312(e)(2)(i).
¹⁰⁶ 45 C.F.R. §164.312(e)(2)(ii).
¹⁰⁷ 45 C.F.R. §160.103.
¹⁰⁸ 45 C.F.R. §164.308(b)(1).
¹⁰⁹ Under 45 C.F.R. §164.308(b)(2), the requirements of the business associate agreement standard do not apply to transmission by a covered entity of ePHI to a health care provider concerning the treatment of an individual; transmission of ePHI by a group health plan, HMO, or health insurer on behalf of a group health plan to a sponsor; or to transmission of ePHI from or to other agencies providing certain services when the covered entity is a health plan that is a government program providing public benefits.
¹¹⁰ 45 C.F.R. §164.314(b) contains standards and implementation specifications applicable to group health plans.

¹¹¹ 45 C.F.R. §164.314(a)(2)(i) or 45 C.F.R. §164.314(a)(2)(ii).

¹¹² Rule 45 C.F.R. §164.314(a)(2)(ii) sets out additional specific *required* provisions if the covered entity and its business associate both are governmental entities. Subsections (b)(1) and (2) of the rule address standards and implementation Specifications for group health plans.

¹¹³ 45 C.F.R. §164.314(a)(2)(i)(A).

¹¹⁴ 45 C.F.R. 164.314(a)(2)(i)(B).

¹¹⁵ 45 C.F.R. 164.314(a)(2)(i)(C).

¹¹⁶ Under 45 C.F.R. §164.314(a)(1)(ii) a covered entity is not in compliance with HIPAA privacy standards in 45 C.F.R. §164.502(e) and 45 C.F.R. §164.314(a) if it knew of a pattern of 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. If such steps were unsuccessful, the covered entity is required to terminate the contract or arrangement, if feasible; or if termination is not feasible, report the problem to the HHS Secretary. Furthermore, a covered entity that violates the satisfactory assurances it provides as a business associate to another covered entity will not be in compliance with this standard and 45 C.F.R. §164.314(a).

¹¹⁷ 45C.F.R. §164.314(a)(2)(i)(D).

¹¹⁸ 45 C.F.R. §164.316 .

¹¹⁹ 45 C.F.R. §164.306(b)(1).

¹²⁰ 45 C.F.R. §164.306(b)(2).

¹²¹ 45 C.F.R. §164.316.

¹²² 45 C.F.R. §164.316(b)(1)(i).

¹²³ 45 C.F.R. §164.316(b)(1)(ii).

¹²⁴ 45 C.F.R. §164.316(b)(2)(i).

¹²⁵ 45 C.F.R. §164.316(b)(2)(ii).

¹²⁶ 45 C.F.R. §164.316(b)(2)(iii).

James M. Barclay is a healthcare attorney practicing in the Tallahassee offices of the Ruden McClosky firm. He represents healthcare providers on regulatory matters such as certificate of need, licensing, Medicaid, and HIPAA. He received a B.S. in journalism from the University of Florida and a J.D. from The Florida State University College of Law. Mr. Barclay is chair of the Health Law Section of The Florida Bar and founder of the 2005 Health Law Institute. He is a director and past president of the Florida Academy of Healthcare Attorneys of the Florida Hospital Association.