HIPAA Privacy and Security: Issues for Employer-Sponsored Health Plans

Mary Leto Pareja
University of New Mexico - Main Campus

Follow this and additional works at: http://digitalrepository.unm.edu/law_facultyscholarship

Recommended Citation
On August 21, 1996, President Bill Clinton signed into law the Health Insurance Portability and Accountability Act ("HIPAA").¹ The first shockwave from HIPAA hit the world of health care in 1998. That was the year Title I of HIPAA generally became effective.² Title I introduced several substantive healthcare reforms, including limiting the application of preexisting condition exclusions, guaranteeing special enrollment rights, prohibiting discrimination based on health status, and guaranteeing the availability and renewability of health insurance in both the group and individual insurance markets.³ HIPAA's second shockwave is currently rolling through the healthcare world, otherwise known as Title II of HIPAA or the "administrative simplification provisions."⁴

HIPAA's administrative simplification provisions include transaction standards for electronic transmission of data, privacy standards, and security standards. The transaction standards (also called electronic data interchange or "EDI" standards) require that certain electronic health care transactions be done in a standardized format.⁵ The EDI standards became effective on October 16, 2002; small plans⁶ and any covered entity that requested an extension had until October 16, 2003 to comply.⁸

The privacy standards define who is authorized to access health information created or maintained by certain covered entities and for what purposes. They also provide individuals with certain rights with respect to their protected health information.⁷ The privacy standards generally became effective April 14, 2003; however, small group health plans had an additional year to comply (until April 14, 2004).⁸

The security standards address the ability to control access to information and protect information from accidental or intentional disclosure to unauthorized persons or unauthorized alteration, destruction, or loss.⁹ The security standards generally are effective April 21, 2005, but small group health plans have an additional year to comply (until April 21, 2006).¹⁰

This article discusses issues about privacy standards and provides an overview of security issues. Some of the privacy issues include who must comply, what information is protected, and permissible disclosure of protected information. The overview of security issues covers administrative, physical, and technical safeguards, as well as organizational requirements. Any practitioner who works with employers that sponsor a health plan for their employees should be aware of these issues, as this is a new area of potential risk for those clients.

**HIPAA Privacy Standards: Linger ing Issues**

A complete discussion of the HIPAA privacy rule is beyond the scope of this article. Instead, this article focuses on some of the more commonly misunderstood issues that frequently arise for employer-sponsored health plans under the HIPAA rule.¹¹

**Who Must Comply**

The first response many employers have to HIPAA is incredulity that this rule might impact them. Common refrains are: "I heard employers aren't subject to HIPAA"; "I'm not subject to ERISA";¹² "I'm fully insured"; "It's just a medical flexible spending account";¹³ and "I'm a small employer." Actually, HIPAA's administrative simplification rules apply to "covered entities," which are (1) health plans, (2) health care clearinghouses, and (3) most healthcare providers.¹⁴

Employers are not covered entities directly. However, the term "health plan" encompasses not only insurance companies, but also employer-sponsored group health plans.¹⁵ Therefore, many employers face a compliance obligation because they maintain a group health plan for their employees. Group health plans include medical, dental, and vision plans; medical flexible spending arrangements; and most employee assistance programs. There are no exceptions for non-ERISA plans, governmental plans, or church plans.

**Exceptions for Small Self-Administered Plans:** There is a complete exclusion for health plans that have fewer than fifty participants and that are completely administered by the sponsoring employer.¹⁶ The HIPAA regulations borrow the ERISA definition of "participant," even for plans that are not subject to ERISA. Therefore, a participant is "any employee or former employee of an employer . . . who is or may become eligible to receive a benefit of any type from an employee ben-
efit plan..." 17 (Emphasis added.) This means that all employees eligible to elect a benefit count toward the fifty-participant threshold, even if the employee does not actually elect the benefit. There is no exception for small plans that are not administered solely by the employer. Therefore, if a third-party administrator is involved, the exception is not available.

Reduced Compliance Burden for Certain Fully-Insured Plans: There is a reduced compliance burden, but not a complete exemption, for fully-insured plans that handle only very limited health information. To qualify for this reduced compliance burden, a plan must provide benefits "solely through an insurance contract with a health insurance issuer or an HMO." 18 Any group health plan that is at least partially self-funded does not qualify for the exception. Therefore, most medical expense reimbursement plans do not qualify for the exception, even though the employer typically has little involvement in such a plan.

In addition, to qualify for reduced compliance burden, the plan must limit the types of health information it may create or receive to the following: (1) enrollment information; (2) summary health information for purposes of obtaining premium bids or amending or terminating the plan; and (3) de-identified health information. 19 Summary health information 20 and de-identified health information 21 in short, comprise health information from which all identifying factors have been scrubbed.

One of the biggest difficulties that plans face in trying to take advantage of the fully-insured plan exception is the information the plan may receive from the participants themselves. The problem arises when a participant asks the employer for help resolving a claims dispute, or for help in navigating the plan, and when the participant reveals details of his or her (or his her dependent's) health that either is or is close to becoming protected health information. To preserve the availability of the fully-insured plan exception, therefore, at this point an employer either must obtain an authorization from the employee to permit it to utilize the information or must direct the employee somewhere else for assistance (such as the insurance company or the broker) and be sure not to "transmit or maintain" the information the employee has shared. A fully-insured plan that intends to use the fully-insured plan exception must ensure that it has procedures in place to help it avoid such potential pitfalls.

Protected Information
The privacy rule safeguards "protected health information," also known as PHI. PHI is "individually identifiable health information" that is transmitted or maintained by a covered entity in any form or media, whether electronic, paper, or oral. 22 "Individually identifiable health information" is information, including demographic data, that:
1) is "created or received by a health care provider, health plan, employer, or health care clearinghouse"; 23
2) "relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual," 24 and
3) identifies the individual or could be used to identify the individual. 25 However, "employment records held by a covered entity in its role as employer" are excluded from protection. 26 This employment records exception applies to employers who also are covered entities, such as hospitals, doctors' offices, or insurance companies.

Enrollment Information: One of the biggest issues for many employers is whether enrollment information is PHI. Enrollment information is clearly individually identifiable health information because it is created or received by an employer and it relates to the payment for health care. The Preamble to the 2002 changes to the final regulations clarify that enrollment information is not protected when held by a plan sponsor, because a plan sponsor is not a covered entity. 27 However, the information becomes protected when the plan receives the information from the plan sponsor.

The problem for most employers is that there is no clear line between the employer and the plan. The people administering the plan are employees of the employer. Clearly, though, the information is transmitted to the plan at some point in time. From that point forward, it is protected under HIPAA.

Disclosure of Protected Health Information
The HIPAA privacy rule defines and limits the circumstances in which an individual's PHI may be used or disclosed by a covered entity. A covered entity may use or disclose PHI only if HIPAA specifically permits that particular use or disclosure or if the individual who is the subject of the information authorizes the use or disclosure in writing. 28 A detailed discussion of the variety of circumstances covered in the HIPAA privacy rule is beyond the scope of this article, but certain situations are more frequently asked about.

Disclosure to Family Members: Many employers, in the spirit of providing good customer service to their employees, were accustomed to discussing health insurance issues with any family member who called and asked about them. HIPAA imposes new restrictions on this practice. Without getting a specific authorization from the subject of the information, only under limited circumstances may a health plan disclose PHI to a family member, close personal friend, or other person identified by the individual. 29

The individual generally must agree (or not object) to the disclosure. 30 In this case, the plan may disclose PHI that is directly relevant to that person's involvement with the individual's care or payment for health care. 31 The plan also may disclose PHI if either (1) the individual is not present and the disclosure cannot wait to obtain consent or (2) the individual is unable to agree or object due to an incapacity or emergency. However, disclosure in this instance is allowed only if the disclosure is in the individual's best interest and is directly related to the other person's involvement in the individual's health care (but not payment for health care). 32

These rules are much more restrictive than that standard with which employers (and employees) are familiar. However, a plan may disclose information to any person if the individual has signed a HIPAA authorization permitting the disclosure. 33 Many employers are responding by making blank HIPAA authorizations readily available to their employees. They also are educating their employees that without an authorization, it is likely that the plan, employer, or any other healthcare vendor will not be able to discuss insurance matters freely with any member of the employee's household.

Using PHI to Prevent Fraud and Abuse: Before the advent of HIPAA privacy standards, some employers had spent many years and dollars integrating their disability programs with their medical plans. The idea was that fraudulent disability claims could be identified if the disability claims were compared against the medical claims. If an employee was claiming disability for a back disorder, for example, but had never submitted a claim to the medical plan for back care, a red
flag was raised on that disability claim. HIPAA threw a monkey wrench into these types of fraud and abuse detection programs.

A health plan (and any of its vendors) can disclose PHI to the employer sponsoring the plan if the employer has signed a plan amendment that (in part) obligates the employer to use the PHI only for the plan administration functions the employer performs for the health plan.34 In other words, PHI from the health plan cannot be used by the employer to help administer the disability plan (or any other benefit program of the employer). The only way this information sharing is permitted is if the employee specifically authorizes the disclosure.35

It seems optimistic to expect an employee who is suspected of filing a fraudulent disability claim to authorize the disclosure of information that could be used to detect the fraud. Covered entities generally may not condition health plan enrollment or benefits on the individual signing an authorization.36 Therefore, the health plan, as a covered entity, cannot penalize the employee for failing to authorize this type of disclosure. However, the disability plan is not a covered entity because it is not a health plan. The disability plan could be written so that payment of benefits is conditioned on the employee’s giving the disability plan an authorization to receive relevant claims information from the health plan. Care needs to be taken that such authorization is valid under HIPAA.37

HIPAA Security Requirements: An Overview

HIPAA's security rule requires that covered entities: (1) maintain or transmit electronic PHI to ensure the integrity, confidentiality, and availability of electronic PHI; (2) protect against reasonably anticipated threats to the security or integrity of electronic PHI; (3) protect against the unauthorized uses or disclosures of electronic PHI; and (4) ensure the workforce is in compliance with the security rule.38 The security rule protects only electronic PHI. “PHI” is defined the same as it is for the privacy rule (see above), and PHI is considered “electronic” when it is transmitted or maintained in electronic media.39

The regulations provide a detailed definition of “electronic media,” and the definition cuts a wide swath. In general, however, the information will not be subject to these rules unless it existed in electronic form before being transmitted.40 Thus, the security rule is not implicated when a covered entity sends a paper fax, but is implicated when a covered entity sends an e-mail.

The security rule sets forth a series of security standards that must be met with respect to electronic PHI. The security standards establish a minimum level of security to be met by covered entities. Each standard is implemented through implementation specifications, and some are mandatory for all covered entities (the regulations call these “required” implementation specifications).41 Other implementation specifications are mandatory only if they are reasonable and appropriate under the circumstances (the regulations call these “addressable” implementation specifications).42 However, if a covered entity decides that an addressable
specification is not reasonable and appropriate, it must document its reasons for that decision and consider equivalent, alternative measures.43

The security standards are intended to be scalable, and covered entities are allowed flexibility in their approach to compliance.44 Thus, what is appropriate for a plan with 5,000 participants may not be appropriate for a plan with fifty participants. However, all covered entities (and employers on behalf of their health plans) must take the time to formally assess their compliance obligations.

The first step in complying with the security requirements is to conduct an assessment of the standards and the implementation specifications in the regulations. Each covered entity must ensure that the standards and mandatory implementation specifications can be satisfied by the compliance deadline. The covered entity then must make an informed decision regarding whether the addressable implementation specifications need to be implemented.

The second step is to develop written policies and procedures that ensure compliance with the security standards and document the decisions made as a result of the assessment.45 The third step is to draft appropriate documentation. As with the privacy rule, written contracts need to be negotiated with all business associates46 and, if a plan sponsor is going to access or maintain electronic PHI, the plan document must be amended to permit this.47

The security standards are divided into three groups: administrative safeguards, physical safeguards, and technical safeguards. Each is discussed below.

While going through these standards, it is important to remember, as noted above, that the standards are scalable. Although all covered entities must go through each step in the process, the resulting policies and procedures should be far less demanding for smaller companies. Also, it is possible to avoid the issue of HIPAA security entirely, or significantly lessen its impact, by outsourcing most or all of the health plan functions. If a covered entity has no or little electronic PHI, its HIPAA security burden is eliminated or reduced. The cost for this reduced burden is a reduced ability to oversee and audit the health plan. Moreover, in this era of double-digit healthcare increases, outsourcing may be too costly for many employers.

**Administrative Safeguards**

Administrative safeguards are defined as the administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.48

The implementation specifications deal with the process for managing security issues, the appointment of security personnel, the implementation of policies and procedures, controlling internal access to information, awareness and training of employees, the process for reporting security incidents, developing a contingency plan, and periodic assessments of the security policies and procedures.

**Security Management Process:** A covered entity must “implement policies and procedures to prevent, detect, contain, and correct security violations.”49 As part of the security management process, covered entities are required to do the following four things:

- **Risk Assessment:** Assess the potential risks and vulnerabilities to electronic PHI.50
- **Risk Management:** Implement security measures to address the risks identified during the risk assessment.51
- **Sanction Policy:** Apply appropriate sanctions against workforce members who violate the security policies and procedures.52
- **Periodic Security Reviews:** Regularly review information system activity.53

**Appoint a Security Official:** Each covered entity must appoint a security official who is responsible for the development and implementation of the required policies and procedures.54 This person need not also be the privacy officer.

**Workforce Security:** A covered entity must implement policies and procedures to ensure that all employees have appropriate access to electronic PHI and to prevent access by unauthorized employees.55 Thus, the covered entity must build a firewall, similar to the privacy requirement.

There are no required implementation specifications. However, if appropriate and reasonable under the circumstances, the covered entity should implement procedures for the authorization and supervision of employees who work with electronic PHI,56 procedures to determine that an employee’s access to electronic PHI is appropriate,57 and procedures for terminating access when the employment ends or when it is determined that an employee’s access is no longer appropriate.58

**Information Access Management:** A covered entity must implement policies and procedures for authorizing appropriate access to electronic PHI.58 In other words, there must be a procedure for including employees in the firewall. If a healthcare clearinghouse (not applicable
to employer-sponsored health plans) is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI from unauthorized access by the larger organizations. If appropriate and reasonable under the circumstances, a covered entity also should implement policies and procedures for granting access to electronic PHI (for example, by granting access to particular workstations or computer programs), for documenting such access, and for reviewing and modifying an employee’s right to access electronic PHI.

Security Awareness and Training: A covered entity must implement a security awareness and training program for all employees. Unlike the privacy rule, security training is not limited to those within the firewall (those with access to electronic PHI). There are no required implementation specifications. However, if appropriate and reasonable under the circumstances, a covered entity must issue periodic security updates and have procedures for guarding against, detecting, and reporting malicious software, for monitoring log-in attempts and reporting discrepancies, and for creating, changing, and safeguarding passwords.

Security Incident Procedures: A covered entity must implement policies and procedures to address security incidents. A security incident is the “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” The policies must include a method to identify and respond to suspected or known security incidents, mitigation provisions, and a requirement that all incidents and outcomes be documented.

Contingency Plan: A covered entity must establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI. The contingency plan must include a data backup plan, disaster recovery plan, and emergency operations plan. If reasonable and appropriate under the circumstances, a covered entity also should periodically test and revise the contingency plan, as well as conduct a data criticality analysis to determine which forms of electronic PHI are necessary for emergency operations.

Evaluation: A covered entity must periodically evaluate its compliance with the security rule. The evaluation must address both technical and non-technical aspects of compliance. The initial evaluation should be based on the security rule standards. Subsequent evaluations should be in response to environmental or operational changes affecting the security of electronic PHI.

Physical Safeguards

The HIPAA security rule requires covered entities to implement physical safeguards to protect the security of electronic PHI. Physical safeguards are physical measures, policies, and procedures, to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

The implementation specifications deal with controlling access to facilities, workstations, hardware, and electronic media.

Facility Access Controls: A covered entity must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed. If reasonable and appropriate under the circumstances, the covered entity’s policies and procedures should include the following: (1) a contingency plan for access in an emergency and to retrieve lost data; (2) a plan to safeguard the facility and equipment from unauthorized physical intrusion; (3) procedures to control and validate a person’s access to facilities, including visitor control; and (4) documentation of security-related facility maintenance or modification.

Workstation Use and Security: For each workstation (or class of workstations) that can access electronic PHI, the policies and procedures must specify the proper functions to be performed at the workstation, the manner in which those functions are to be performed, and the physical attributes of the surroundings of the workstation. The covered entity then must implement physical safeguards for those workstations to restrict access to authorized users.

Device and Media Controls: A covered entity must implement policies and procedures regarding the movement of hardware and electronic media that contain electronic PHI into, out of, and within a facility. These policies and procedures must contain instructions on how to dispose of electronic PHI (and hardware or media on which it is stored), as well as removal of electronic PHI from electronic media before reuse of the media. If reasonable and appropriate under the circumstances, the covered entity’s policies and procedures also should require that movements of hardware and electronic media be recorded. Further, it should address data backup and storage requirements before equipment is moved.

Technical Safeguards

The security rule prescribes technical safeguards to protect electronic PHI. Technical safeguards are the technology and the policies and procedures for its use that protect electronic protected health information and control access to it.

The implementation specifications deal with information systems issues, such as controlling access to information systems, recording and auditing system activity, maintaining the system’s integrity, and preventing authorized access or interception.

Access Control: A covered entity must employ technology that restricts access to information systems that maintain electronic PHI. This technology must include a unique user identification system. The covered entity also must have procedures for obtaining necessary electronic PHI during an emergency. If appropriate and reasonable under the circumstances, the technology employed should include an automatic log-off procedure (whereby a user will be logged off after a pre-determined time of inactivity) and a mechanism to encrypt and decrypt electronic PHI.

Audit Controls: A covered entity must implement a system (using hardware, software, and/or procedural mechanisms) to record and examine activity in information systems that store or use electronic PHI. For example, they must have the capacity to monitor which databases or files are accessed by which users and actually monitor the activity to ensure that only authorized users are accessing electronic PHI.

Integrity Standard: A covered entity must implement policies and procedures to protect electronic PHI from improper alteration or destruction. If reasonable and appropriate under the circumstances, electronic mechanisms should be used to corroborate that electronic PHI has not been improperly altered or destroyed.

Person or Entity Authentication: A covered entity must verify the identity of a person or entity seeking access to electronic PHI. For example, passwords or
digital signature technology may be employed to verify identity.

**Transmission Security:** A covered entity must employ technology to protect electronic PHI that is being transmitted over an electronic communications network from being intercepted.\(^\text{101}\) If reasonable and appropriate under the circumstances, the technology employed should ensure that electronic PHI is not improperly modified.\(^\text{102}\) Electronic PHI should be encrypted whenever it is deemed appropriate.\(^\text{103}\)

**Organizational Requirements**

In addition to the standards set forth in the regulations that impact a covered entity's security policies and procedures, there are additional documentation requirements. These include business associate contracts, plan amendments, and document retention policies.

**Business Associate Contracts:** Each covered entity should have already negotiated an agreement with its business associates that addresses privacy issues.\(^\text{104}\) A business associate, in general, is a third party who performs services for the covered entity.\(^\text{105}\) For example, the third-party administrator of a self-funded health plan is a business associate of the plan. These business associate agreements need to be amended (or supplemented) to address security standards.\(^\text{106}\) The agreement must obligate the business associate to do the following:

1. "Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic [PHI] that it creates, receives, maintains, or transmits on behalf of the covered entity in compliance with [the HIPAA security rule]."\(^\text{107}\)
2. "Ensure that any agent, including a subcontractor, to whom it provides [electronic PHI] agrees to implement reasonable and appropriate safeguards to protect the information."\(^\text{108}\)
3. "Report to the covered entity any security incident of which it becomes aware."\(^\text{109}\)

As with the privacy rule, the business associate contract must permit the covered entity to terminate the contract on a material breach by the business associate.\(^\text{110}\) Finally, as with the privacy rule, if the covered entity becomes aware of a material breach by the business associate, the covered entity must terminate the contract, if feasible, when the business associate fails to cure the breach or end the violation.\(^\text{111}\)

**Plan Amendment:** If the plan sponsor of a health plan has access to or maintains electronic PHI, the plan sponsor must amend the plan document to ensure appropriate security measures are taken.\(^\text{112}\) The only exceptions are if the plan qualifies to use the fully insured plan exception (see above) or if the information is maintained or transmitted pursuant to a HIPAA authorization.\(^\text{113}\) The plan document must obligate the plan sponsor to do the following:

1. "Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic [PHI] that it creates, receives, maintains, or transmits on behalf of the group health plan."\(^\text{114}\)
2. Ensure that the privacy firewall is "supported by reasonable and appropriate security measures" to protect electronic PHI;\(^\text{115}\)
3. "Ensure that any agent, including a subcontractor, to whom it provides [electronic PHI] agrees to implement reasonable and appropriate safeguards to protect the information."\(^\text{116}\) and
4. "Report to the group health plan any security incident of which it becomes aware."\(^\text{117}\)

**Document Retention:** Any documentation that is required under the security rule, including the security policies and procedures themselves, must be retained in certain ways. They must be maintained in writing, retained for a minimum of six years, be made available to persons responsible for implementation, and be reviewed periodically and updated as needed in response to environmental or operational changes.\(^\text{118}\)

**Conclusion**

Although the compliance deadline for the HIPAA privacy rule has already come and gone, HIPAA privacy compliance is an ongoing process. Virtually all employers are impacted in some manner. It is never too late to begin the compliance process or to ensure that the steps taken are adequate to protect the employer and the plan from liability. The deadline for the HIPAA security rule is just around the corner (April 2005) for all covered entities except small health plans. Compliance requires some lead time to perform the required assessments, to make appropriate technology decisions, and to implement any required changes. Now is the time to begin the process.

**NOTES**

2. HIPAA's portability, special enrollment, and nondiscrimination provisions, as well as the guaranteed availability and renewability rules for the group insurance market, were effective for plan years beginning on or after July 1, 1997. HIPAA §§ 101(g), 102(c), and 401(c).
4. See generally 45 C.F.R. Part 162.
5. A "small health plan" is defined as a health plan with annual receipts of $5 million or less. 45 C.F.R. § 160.103. Annual receipts are insurance premiums for insured plans or claims paid for self-funded plans. See "HHS Frequently Asked Questions ("How should a health plan determine what receipts to use to decide whether it qualifies as a small health plan?")."
6. 45 C.F.R. § 162.900.
7. See generally 45 C.F.R. Part 164, Subpart E.
8. 45 C.F.R. § 164.534.
9. See generally 45 C.F.R. Part 164, Subpart C.
10. 45 C.F.R. § 164.318.
12. The Employee Retirement Income Security Act of 1974, Pub. L. 93-406 (Sept. 2, 1974), as amended (hereafter, "ERISA"), which is a comprehensive federal law that regulates pensions and other employee benefits maintained by many, but not all, employers.
14. 45 C.F.R. § 160.103.
15. Id.
16. Id.
17. ERISA § 3(7).
18. 45 C.F.R. § 164.530(k)(i).
19. 45 C.F.R. § 164.530(k)(ii); 45 C.F.R. § 164.530(x)(1).
20. "Summary health information" means information (that may be individually identifiable health information), which summarizes the claims history, claims expenses, or type of...
claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan. The following identifiers must be removed from the information (this is the same list as for deidentified information, except more geographic information can be included):

1) names
2) geographic subdivisions smaller than a five-digit zip code
3) month and day of birth and other personal dates
4) ages over 89
5) telephone and fax numbers
6) electronic mail addresses
7) Social Security numbers
8) medical record numbers
9) health plan beneficiary numbers
10) account numbers
11) certificate or license numbers
12) vehicle identifiers (including serial and license plate numbers)
13) device identifiers and serial numbers
14) Web universal resource locators (URLs)
15) biometric identifiers (such as finger- or voice-prints)
16) full-face photographic images
17) any other unique identifying numbers, characteristics, or codes.

45 C.F.R. § 164.504(a).

21. "Deidentified information" means health information that does not include, for the individual or the individual’s relatives, employers, or household members, any of the identifiers listed in note 20, supra, except that geographic subdivisions must be deleted if smaller than a state. In lieu of deleting these specific items of information, a set of health information also is considered deidentified if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (1) applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (2) documents the methods and results of the analysis that justify such determination. 45 C.F.R. § 164.514(b).

22. 45 C.F.R. § 160.103. Actually, the regulations do not specify that protected health information is limited to information maintained or transmitted by covered entities. However, the preamble to the 2000 final regulations makes it clear that the government intended to make such a distinction. The Preamble states: “We use the phrase ‘protected health information’ to distinguish between the individually identifiable health information that is used or disclosed by the entities that are subject to this rule and the entire universe of individually identifiable health information.” 65 Fed. Reg. 82461, 82612 (Dec. 28, 2000).

23. Id.
24. Id.
25. Id.
26. Id.
28. 45 C.F.R. § 164.502(a).
29. 45 C.F.R. §§ 164.510(b) and 164.508(a) (1).
30. 45 C.F.R. § 164.510(b)(2).
31. 45 C.F.R. § 164.510(b)(1).
32. 45 C.F.R. § 164.510(b)(3).
33. 45 C.F.R. § 164.508(a)(1).
34. 45 C.F.R. § 164.504(f).
35. 45 C.F.R. § 164.508(a)(1).
36. 45 C.F.R. § 164.508(b)(4).
37. 45 C.F.R. § 164.508(c).
38. 45 C.F.R. § 164.306(a).
39. 45 C.F.R. § 160.103.
40. "Electronic media means: (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dialup lines, private networks, and the physical movement of removable/transportable electronic storage me-
via facsimile, and of voice, via telephone, are not considered to be transmissions by electronic media, because the information being exchanged did not exist in electronic form before the transmission. 45 C.F.R. § 164.308(a).

41. 45 C.F.R. § 164.308(d).
42. Id.
43. 45 C.F.R. § 164.306(d)(3).
44. 45 C.F.R. § 164.306(b).
45. 45 C.F.R. § 164.316(a).
46. 45 C.F.R. § 164.314(a).
47. 45 C.F.R. § 164.314(b).
48. 45 C.F.R. § 164.304.
49. 45 C.F.R. § 164.308(a)(1).
50. 45 C.F.R. § 164.308(a)(1)(i).
51. 45 C.F.R. § 164.308(a)(1)(ii).
52. 45 C.F.R. § 164.308(a)(1)(ii)(A).
53. 45 C.F.R. § 164.308(a)(1)(ii)(B).
54. 45 C.F.R. § 164.308(a)(2).
55. 45 C.F.R. § 164.308(a)(3).
56. 45 C.F.R. § 164.308(a)(3)(i).
57. 45 C.F.R. § 164.308(a)(3)(ii).
58. 45 C.F.R. § 164.308(a)(3)(iii).
59. 45 C.F.R. § 164.308(a)(4).
60. 45 C.F.R. § 164.308(a)(4)(i).
61. 45 C.F.R. § 164.308(a)(4)(ii).
62. 45 C.F.R. § 164.308(a)(5).
63. 45 C.F.R. § 164.308(a)(5)(i).
64. 45 C.F.R. § 164.308(a)(5)(ii).
65. 45 C.F.R. § 164.308(a)(5)(ii)(A).
66. 45 C.F.R. § 164.308(a)(5)(ii)(B).
67. 45 C.F.R. § 164.308(a)(5)(ii)(C).
68. 45 C.F.R. § 164.308(a)(5)(ii)(D).
69. 45 C.F.R. § 164.308(a)(6).
70. 45 C.F.R. § 164.308(a)(7).
71. 45 C.F.R. § 164.308(a)(7)(i).
72. 45 C.F.R. § 164.308(a)(7)(ii).
73. 45 C.F.R. § 164.308(a)(7)(iii).
74. 45 C.F.R. § 164.308(a)(7)(iv).
75. 45 C.F.R. § 164.308(a)(7)(v).
76. 45 C.F.R. § 164.308(a)(7)(vi).
77. Id.
78. Id.
79. Id.
80. 45 C.F.R. § 164.304.
81. 45 C.F.R. § 164.310(a)(1).
82. 45 C.F.R. § 164.310(a)(2).
83. 45 C.F.R. § 164.310(a)(2)(i).
84. 45 C.F.R. § 164.310(a)(2)(ii).
85. 45 C.F.R. § 164.310(a)(2)(iii).
86. 45 C.F.R. § 164.310(a)(2)(iv).
87. 45 C.F.R. § 164.310(a)(3).
88. 45 C.F.R. § 164.310(a)(4).
89. 45 C.F.R. § 164.310(b).
90. 45 C.F.R. § 164.310(c).
91. 45 C.F.R. § 164.310(d).
92. 45 C.F.R. § 164.310(d)(1).
93. 45 C.F.R. § 164.310(d)(2).
94. 45 C.F.R. § 164.310(d)(3).
95. 45 C.F.R. § 164.310(d)(4).
96. 45 C.F.R. § 164.310(e).
97. 45 C.F.R. § 164.310(e)(1).
98. 45 C.F.R. § 164.310(e)(2).
99. 45 C.F.R. § 164.310(e)(3).
100. 45 C.F.R. § 164.310(e)(4).
101. 45 C.F.R. § 164.310(f).
102. 45 C.F.R. § 164.310(g).
103. 45 C.F.R. § 164.310(h).
104. 45 C.F.R. § 164.310(i).
105. The regulations generally define the term "business associate" as a person who, on behalf of a covered entity, but other than in the capacity of a member of the workforce of the covered entity, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by [HIPAA's administrative simplification rules]; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in [45 C.F.R. § 164.501]), management, administrative, accreditation, or financial services to or for such covered entity, . . . where the provision of the service involves the disclosure of individually identifiable health information from such covered entity . . . , or from another business associate of such covered entity or arrangement, to the person.

A covered entity may be a business associate of another covered entity in certain situations. 45 C.F.R. § 160.103.

106. 45 C.F.R. § 164.314(a)(1)(ii). If both the covered entity and the business associate are governmental entities, different requirements apply. See 45 C.F.R. § 164.314(a)(2)(ii).