Pain Physician. 2003;6:377-381, ISSN 1533-3159

PRACTICE MANAGEMENT

AND YOU THOUGHT YOU WERE DONE WITH HIPAA: COMPLYING WITH THE NEW SECURITY RULE

Erin Brisbay McMahon, JD

On February 20, 2003, the Department of Health and Human Services (HHS), pursuant to its authority under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), issued the final rule on Security Standards for electronic protected health information (PHI). The rule addresses the duties of providers who conduct electronic transactions covered under the HIPAA transactions and code sets rule to address the security issues surrounding the storage and transmission of electronic PHI.

Providers who are required to comply with the security rule must do so by April 20, 2005. While this may seem like a long time, the compliance requirements are lengthy and burdensome, so providers would be well advised to start compliance efforts now. Appointing a security officer and beginning a risk analysis should be the first priorities of any practice. While the security officer will be integral in a practice's compliance, it is ultimately the burden of the practice to ensure compliance with the rule.

Penalties for non-compliance are stiff: civil money penalties of up to a $100 fine for every violation of each requirement or prohibition, capped at $25,000 per year for all violations of an identical requirement or prohibition. Criminal penalties must be imposed if a person knowingly and in violation of the security rule: obtains individually identifiable health information relating to an individual or discloses individually identifiable information to another person.

This article is not, and should not be construed as, legal advice or an opinion on specific situations.

Keywords: HIPAA, security standards, required, addressable

While many providers were busy putting the finishing touches on their Health Insurance Portability and Accountability Act (HIPAA) privacy compliance program and gearing up to comply with the HIPAA transactions and code sets rules, the Department of Health and Human Services (HHS) was busy polishing the last draft of the security standards for electronic health information. On February 20, 2003, HHS issued the final HIPAA security rules (1). These rules govern how physicians and other health care providers who conduct electronic transactions covered under the HIPAA transactions and code sets rule, as well as health plans and health care clearinghouses, deal with the security issues surrounding the storage and transmission of electronic health care information. Basically, if a provider or a practice determined that it was a covered entity under HIPAA and needed to comply with the HIPAA privacy rule, then those providers and practices must comply with the HIPAA security rule. If a provider or practice is still unsure if it is required to comply with HIPAA, a decision tree that will help to determine whether it is required to comply with HIPAA is available at: *http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp*

Providers who must comply with the security rule have until April 20, 2005 (2) to achieve compliance. This article will describe a basic roadmap for compliance, but is not intended as a substitute for reading the rule and consulting legal counsel with respect to specific situation(s).

SETTING A HIGH STANDARD

The HIPAA security rules require providers to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (PHI) the provider creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA privacy rule; and
- Ensure compliance with the security rule by its workforce (employees, students and trainees, and volunteers) (3).

The words "ensure" and "any" should catch your attention. The plain language of the security rule contemplates that providers will take all steps necessary to make sure electronic PHI that providers create, receive, maintain, or transmit in the practice will be kept secure, that providers will have built an electronic fortress (and a physical fortress around electronic equipment) such that no reasonably anticipated threat cannot be rebuffed or dealt with (therefore, providers also need sufficient redundancy for data storage), and that the staff will be thoroughly trained on the security rule. While HHS insists that "'ensuring' protection" does not mean "providing protection, no matter how expensive," it does maintain that providers must "take steps, to the best of [their] ability, to protect [electronic PHI]." HHS states that, "[t]his will involve establishing a balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of" the provider (4).

Although HHS pays homage to the scalability concept, the reality of the security rule is that the adequacy of your security measures will probably only be evaluated when a catastrophic loss has already occurred (e.g., a hacker has pub-

From Wyatt, Tarrant & Combs, LLP, Lexington, KY. Address Correspondence: Erin Brisbay McMahon, Esq, 250 W. Main St., Suite 1600, Lexington, Kentucky 40507. E-mail: emcmahon@wyattfirm.com
Funding: There was no external funding in preparation of this manuscript.

lished your patient records on the internet or, even worse, your staff intentionally or unintentionally does the same thing). The only comforting news here is that the rule itself requires that you take into account the following factors when deciding which security measures to use:

- The size, complexity, and capabilities of your practice;
- The practice's technical infrastructure, hardware, and software security capabilities;
- The costs of the security measures; and
- The probability and criticality of potential risks to electronic PHI (5).

What's more, the rule requires periodic review and modification of security measures to keep up with the times, so that all measures are always "reasonable and appropriate" in response to the threats from hackers and other quarters (6).

Safeguards

The security rule requires establishment of administrative, physical, and technical safeguards to protect electronic PHI. These safeguards consist of standards, which are mandatory when they appear without "implementation specifications," or instructions as to how to implement the standard (the thought being that standards without implementation specifications are self-explanatory). Some standards contain implementation specifications that are either "required" or "addressable." A "required" implementation specification is mandatory. If an implementation specification is labeled "addressable," a provider must assess whether the specification is reasonable and appropriate in its practice environment (when judged against the specification's likely contribution towards protecting electronic PHI), and then either (a) implement the specification or (b) document why it would not be reasonable and appropriate to implement the specification and then implement an equivalent alternative safeguard if reasonable and appropriate (7). A matrix at the end of the security rule will tell you whether any particular safeguard standard or implementation specification is required or addressable (8).

The silver lining to this cloud is that, the privacy rule, required providers to adopt appropriate administrative, physical, and technical safeguards to protect the privacy of all PHI, not just in electronic form (9). Thus, providers and practices should well be on their way to compliance with the security rule.

Required Administrative Safeguards.

Listed below are required standards and implementation specifications:

- *Appointment of a Security Officer.* This person should be an employee who is responsible for the development and implementation of security policies and procedures (10). It is critical that this person have the support of and be able to work with management. Management and the security officer should work together to develop a budget for implementing the security rule.
- *Risk Analysis.* The very first task that should be delegated to the security officer is a risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the practice (11). Based on financial feasibility, an independent firm may perform this analysis. Any information technology (IT) or information systems (IS) person employed by the practice may not, of course, want to point out deficiencies in firewalls that they maintain, nor does the safety and security officer want to point out that the back door is left unlocked some weekends for the convenience of employees. Any consultant employed should be creative and should be able to assess not only the security of the electronic systems but also the adequacy of the building security and the astuteness of all employees in comparison to the security rule standards. For example, the consultant should try several times to pass through the reception area of a practice and get access to the office without speaking to anyone to assess employee reaction. Consultants should also call the office and impersonate an employee who is working from home and supposedly has forgotten his/her password. Consultants should have access to the office to see if, for example, passwords are written down within easy reach of computer monitors.
- Based on necessity or desire to perform risk analysis internally, the preamble to the security rule suggests a review of NIST SP 800-30, "Risk Management Guide for Information Technology Systems," January 2002 (available at *http://csrc.nist.gov/publications/nistpubs/*) (12).

  HHS does state that a "thorough and accurate" risk analysis will consider "'all relevant losses' that would be expected to occur if the security measures were not in place. These would include "losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. (13)"
- *Policies and Procedures.* The practice must document and implement policies and procedures to prevent, detect, contain, and correct security violations (14). This is best done by the security officer after the risk analysis and in conjunction with risk management. Policies must address workforce access to electronic PHI (15).
- *Risk Management.* The practice must implement security measures sufficient to reduce risks and vulnerabilities identified in the risk analysis (16).
- *Sanction policy.* The security officer, in conjunction with the human resources director, must develop a sanction policy for workforce members that fail to comply with the security policies and procedures (17). While sanctions may be progressive depending on the severity of the violation, they should be strictly enforced. The sanction policy should allow the practice to terminate an employee for a first infraction (e.g., selling electronic PHI).
- *Information System Activity Review.* The practice must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports (18). "Security incidents" are defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system"(19). Usually this refers to attempted or successful hacking.

- *Response and Reporting.* The practice must identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the practice; and document security incidents and their outcomes (20).
- *Data Backup Plan.* The practice must establish and implement procedures, if it has not done so already, to create and maintain retrievable exact copies of electronic PHI (21).
- *Disaster Recovery Plan.* The practice must establish (and implement if necessary) procedures to restore lost data (22).
- *Emergency Mode Operation Plan.* The practice must establish (and implement if necessary) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode (23).
- *Business Associate Agreements.* The proposed security rule referred to "chain of trust agreements." The final rule eliminates those, but requires additional language in business associate agreements that you may have already signed pursuant to the privacy rule (24). The extra statements that the security rule will require in business associate agreements for the business associates that create, receive, maintain or transmit electronic PHI on your behalf are as follows (25):
  - The business associate must agree to 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 practice as required by the security rule;
  - The business associate must agree to ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
  - The business associate must agree to report to the practice any security incident of which it becomes aware;
  - The contract must authorize termination by the practice, if the practice determines that the business associate has violated a material term of the business associate contract (actually, this is already required by the privacy rule and so should already be in your business associate agreements).

Business associate agreements must be written (26). Many practices have already entered into business associate agreements with business associates who handle electronic PHI on their behalf and will no doubt be frustrated at having to amend these agreements so soon after executing them. Practices should consider waiting until the last contract renewal date before April 20, 2005 or January 2005, whichever comes first, before revising business associate contracts. HHS might relent on some of these requirements. In any event, your business associates will want to wait until the last possible moment before signing an agreement that requires them to report all of their security incidents to you.

However, providers are not required to enter into business associate agreements to comply with the security rule if:

- The provider is receiving or transmitting electronic PHI to another health care provider for treatment of an individual;
- A group health plan, or an HMO or health insurance issuer on behalf of a group health plan, transmits electronic PHI to the practice as plan sponsor, provided that the requirements of 45 CFR 164.314(b) and 164.504(f) apply and are met (27).
- Evaluation. Practices must perform a periodic technical and nontechnical evaluation, based initially on the standards implemented by the practice under the security rule and subsequently in response to environmental or operational changes affecting the security of electronic PHI (28).

Addressable Administrative Safeguards

Again, the practice should assess whether the following implementation specifications are reasonable and appropriate in its environment (when judged against the specification's likely contribution towards protecting electronic PHI), and then either (a) implement the specification or (b) document why it would not be reasonable and appropriate to implement the specification and then implement an equivalent alternative safeguard if reasonable and appropriate.

- *Authorization/Supervision of Workforce Members.* The practice should assess whether to implement procedures that require workforce members who work with electronic PHI or in locations where it might be accessed to either have authorization to access that PHI and those areas or be supervised while they are doing so (29). A thoughtful approach to this addressable safeguard would include reviewing and if necessary revising the minimum necessary policies that the practice adopted under the HIPAA privacy rule.
- *Workforce Clearance Procedure.* The practice should assess whether to implement procedures to determine that the access of a workforce member to electronic PHI is appropriate (30). This is probably an item that should be addressed in minimum necessary compliance under the privacy rule. HHS has stated that background checks of employees and other workforce members are not required under this implementation specification (31).
- *Termination Procedures.* The practice should assess whether to implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by determinations made under the workforce clearance procedure above (32). This would include implementing procedures for revoking passwords and taking back an employee's keys on termination.
- *Access Authorization.* The practice should assess whether to implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism (33). Again, this probably requires a thorough review of minimum necessary policies and procedures (with some documentation under the privacy rule as to which workforce members have access to what PHI).
- *Access Establishment and Modification.* The practice should assess whether to implement policies

and procedures that, based upon the practice's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process (34).
- *Security Reminders.* Periodic security updates, such as e-mails or newsletters, to the practice's workforce should be provided (35).
- *Protection from Malicious Software.* Procedures for guarding against, detecting, and reporting malicious software (36), such as worms or viruses.
- *Log-in Monitoring.* Procedures for monitoring log-in attempts and reporting discrepancies (37).
- *Password Management.* Procedures for creating, changing, and safeguarding passwords (38).
- *Testing and Revision Procedures.* Procedures for periodic testing and revision of contingency plans, such as data backup, disaster recovery, and emergency mode operations (39).
- *Applications and Data Criticality Analysis.* Procedures for assessment of the relative criticality of specific applications and data in support of other contingency plan components (40).

Required Physical Safeguards

- *Workstation Use.* 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 PHI must be implemented (41). One example would be a requirement for all workforce members to report viruses or worms on their workstations (which include laptops) to the security officer.
- *Workstation Security.* Physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users must be implemented (42).
- *Disposal.* Policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored must be implemented (43). An example would be to adopt a policy and procedure requiring erasure of computer hard drives before sale, donation, return to a lessor, or any other disposal.
- *Media Re-use.* Procedures for removal of electronic PHI from electronic media before the media are made available for re-use must be implemented (44).

Addressable Physical Safeguards

- *Contingency Operations.* Providers must assess the need for proceduresthat 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 (and implemented as needed) (45).
- *Facility Security Plan.* Providers must assess the need for policies and procedures to safeguard the practice and the practice's equipment from unauthorized physical access, tampering, and theft (46).
- *Access Control and Validation Procedures.* Providers must assess the need for 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 (47).
- *Maintenance Records. Providers must assess the need for the* policies and procedures to document repairs and modifications to the physical components of the practice which are related to security (for example, hardware, walls, doors, and locks) (48).
- *Accountability.* Providers must assess the need for a record of the movements of hardware and electronic media and any person responsible for said movements (49).
- *Data Backup and Storage.* Providers must assess the need for a retrievable, exact copy of electronic PHI, when needed, before movement of equipment (50).

Required Technical Safeguards

- *Unique User Identification.* A unique name and/or number for identifying and tracking user identity must be assigned (51).
- *Emergency Access Procedure.* Procedures for obtaining necessary electronic PHI during an emergency must be established (and implemented as needed) (52).
- *Audit Controls.* Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI must be implemented (53).
- *Person or Entity Authentication.* Procedures to verify that a person or entity seeking access to electronic PHI is the one claimed must be implemented(54).

Addressable Technical Safeguards

- *Automatic Logoff.* Providers must assess the need for electronic procedures that terminate an electronic session after a predetermined time of inactivity (55).
- *Encryption and Decryption.* Providers must assess the need for a mechanism to encrypt and decrypt electronic PHI (56).
- *Mechanism to Authenticate Electronic PHI.* Providers must assess the need for electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner (57).
- *Integrity Controls.* Providers must assess the need for security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of (58).
- *Encryption.* Providers must assess the need for a mechanism to encrypt electronic PHI whenever deemed appropriate (59).

Document, Document, and Document

The security rule requires providers to document their security policies and procedures and document changes to the policies and procedures (60). It also requires that practices document actions, activities, and assessments when the rule requires (61). It would be prudent, however, to document all thought processes about implementation of the rule; if HHS appears at a practice's door after a complaint and all that practice can say is that everyone knows and understands the practice's security procedures and why the particular procedures were adopted, the possibility of the practice of incurring a huge civil money penalty are significant. All documentation required by the secu-

rity rule must be kept for six years from the date it was created or was last in effect, whichever is later (62). The documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains (63). It would be even better to allow all members of the workforce access to all the security policies and procedures, since arguably everyone in the practice is responsible for ensuring compliance with the security rule. Policies and procedures must be reviewed periodically and updated in response to environmental and operational changes affecting the security of electronic PHI (64).

Enforcement

HIPAA gives the Secretary of HHS the authority to impose monetary penalties for failure to comply with any requirement or prohibition in the security standards. The Secretary may impose penalties of not more than $100 per violation on any person or entity who fails to comply with a requirement or prohibition. However, the total amount imposed on any one person in each calendar year cannot exceed $25,000 for multiple violations of any one requirement or prohibition (65). Criminal penalties of up to $50,000 and up to one year in prison or both must be imposed if a person knowingly and in violation of the security rule: obtains individually identifiable health information relating to an individual or discloses individually identifiable information to another person. These penalties increase to up to $100,000 and up to five years in prison or both if the information was obtained under false pretenses, and up to $250,000 and up to ten years in prison or both if the violation involves commercial advantage, personal gain, or malicious harm (66).

HIPAA press releases and Fact Sheets can be accessed at *http://www.hhs.gov/ocr/hipaa/*.

Author Affiliation:
Erin Brisbay McMahon, JD
Wyatt, Tarrant & Combs, LLP
250 W. Main St., Suite 1600,
Lexington, Kentucky 40507
E-mail: emcmahon@wyattfirm.com

References

1. 68 Fed. Reg. 8,334.
2. 45 C.F.R. 164.318(c).
3. 45 C.F.R. 164.306(a).
4. 68 Fed. Reg. 8,346.
5. 45 C.F.R. 164.306(b).
6. 45 C.F.R. 164.306(e), 164.308(a)(8).
7. 45 C.F.R. 164.306(d)(3).
8. 68 Fed. Reg. 8,380.
9. 45 C.F.R. 164.530(c).
10. 45 C.F.R. 164.308(a)(2).
11. 45 C.F.R. 164.308(a)(1)(ii)(A).
12. 68 Fed. Reg. 8,346.
13. 68 Fed. Reg. 8,347.
14. 45 C.F.R. 164.308(a)(1)(i), 164.316(b)(1)(i).
15. 45 C.F.R. 164.308(a)(3)(i).
16. 45 C.F.R. 164.308(a)(1)(ii)(B).
17. 45 C.F.R. 164.308(a)(1)(ii)(C).
18. 45 C.F.R. 164.308(a)(1)(ii)(D).
19. 45 C.F.R. 164.304.
20. 45 C.F.R. 164.308(a)(6)(ii).
21. 45 C.F.R. 164.308(a)(7)(ii)(A).
22. 45 C.F.R. 164.308(a)(7)(ii)(B).
23. 45 C.F.R. 164.308(a)(7)(ii)(C).
24. 45 C.F.R. 164.308(b), 164.314(a).
25. 45 C.F.R. 164.314(a)(2).
26. 45 C.F.R. 164.308(b)(4).
27. 45 C.F.R. 164.308(b)(2).
28. 45 C.F.R. 164.308(a)(8).
29. 45 C.F.R. 164.308(a)(3)(ii)(A).
30. 45 C.F.R. 164.308(a)(3)(ii)(B).
31. 68 Fed. Reg. 8,348.
32. 45 C.F.R. 164.308(a)(3)(ii)(C).
33. 45 C.F.R. 164.308(a)(4)(ii)(B).
34. 45 C.F.R. 164.308(a)(4)(ii)(C).
35. 45 C.F.R. 164.308(a)(5)(ii)(A).
36. 45 C.F.R. 164.308(a)(5)(ii)(B).
37. 45 C.F.R. 164.308(a)(5)(ii)(C).
38. 45 C.F.R. 164.308(a)(5)(ii)(D).
39. 45 C.F.R. 164.308(a)(7)(ii)(D).
40. 45 C.F.R. 164.308(a)(7)(ii)(E).
41. 45 C.F.R. 164.310(b).
42. 45 C.F.R. 164.310(c).
43. 45 C.F.R. 164.310(d)(2)(i).
44. 45 C.F.R. 164.310(d)(2)(ii).
45. 45 C.F.R. 164.310(a)(2)(i).
46. 45 C.F.R. 164.310(a)(2)(ii).
47. 45 C.F.R. 164.310(a)(2)(iii).
48. 45 C.F.R. 164.310(a)(2)(iv).
49. 45 C.F.R. 164.310(d)(2)(iii).
50. 45 C.F.R. 164.310(d)(2)(iv).
51. 45 C.F.R. 164.312(a)(2)(i).
52. 45 C.F.R. 164.312(a)(2)(ii).
53. 45 C.F.R. 164.312(b).
54. 45 C.F.R. 164.312(d).
55. 45 C.F.R. 164.312(a)(2)(iii).
56. 45 C.F.R. 164.312(a)(2)(iv).
57. 45 C.F.R. 164.312(c)(2).
58. 45 C.F.R. 164.312(e)(2)(i).
59. 45 C.F.R. 164.312(e)(2)(ii).
60. 45 C.F.R. 164.316(b)(1)(i).
61. 45 C.F.R. 164.316(b)(1)(ii).
62. 45 C.F.R. 164.316(b)(2)(i).
63. 45 C.F.R. 164.316(b)(2)(ii).
64. 45 C.F.R. 164.316(b)(2)(iii).
65. 42 U.S.C. § 1320d-5.
66. 42 U.S.C. § 1320d-6.