HIPAA Security Rule Compliance Deadline Nine Months Away: Tips for Compliance

WIGGIN AND DANA
Counsellors at Law

HIPAA Practice Group Principal Contacts

Jeanette C. Schreiber, Chair
203.498.4334/jschreiber@wiggin.com

Catherine P. Baatz
860.297.3748/cbaatz@wiggin.com

Michelle Wilcox DeBarge
860.297.3702/mdebarge@wiggin.com

Mark W. Heaphy
203.498.4356/mheaphy@wiggin.com

Amanda Littell
203.498.4529/alittell@wiggin.com

Alyssa B. Moss
860.297.3723/amoss@wiggin.com

Mary R. Norris
203.498.4377/mnorris@wiggin.com

Maureen Weaver
203.498.4384/mweaver@wiggin.com

Jennifer N. Willcox
203.498.4396/jwillcox@wiggin.com

The compliance deadline for HIPAA's Security Rule is April 21, 2005 for all covered entities, except small health plans which have until April 21, 2006. Although the deadline is approximately nine months away, there are many tasks involved in bringing your organization into compliance, and it is important to start now if you haven't done so already. This Advisory is intended to give you some helpful tips on how to ensure compliance with all of the Rule's legal requirements.

Background

While the HIPAA Privacy Rule covers protected health information (PHI) in all forms, the HIPAA Security Rule applies only to PHI that is maintained or transformed in electronic form (EPHI). The Security Rule is intended to ensure that covered entities meet the following four objectives:

1) Ensure the confidentiality, integrity and availability of all EPHI that the entity creates, receives, maintains, or transmits;

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and

4) Ensure compliance by the entity's workforce.

Over the next several months you will need to conduct a security assessment that is linked to specific Security Rule requirements; this process will be similar to the one undertaken to comply with the Privacy Rule. You will need to implement various controls, including many administrative policies and procedures to prevent, detect, and correct security violations related to EPHI.

The Security Rule does not spell out specific technical measures that must be followed, but instead establishes categories of administrative, physical, and technical standards and "required" and "addressable" implementation specifications to guide compliance. These standards and specifications give covered entities a more detailed picture of how to comply, but the Rule allows flexibility in choosing the most appropriate measures for a particular entity. This means that you must thoroughly assess your existing security controls to determine which safeguards will best meet the organization's needs from a financial and risk perspective, while also satisfying the Rule's many requirements.

You will need to identify, categorize, and quantify security risks to EPHI and the measures currently in place to address them. You must also consider the organization's size and complexity, its technical infrastructure of systems that maintain EPHI, and the resources available to implement additional security measures outlined in the Rule. This process is at its core a risk-benefit analysis that weighs the operational feasibility and impact of implementing additional security measures against the estimated degree and magnitude of risk (legal and otherwise) attendant to foregoing the additional safe-

continued

HIPAA Security Rule Compliance Deadline Nine Months Away: Tips for Compliance

guards. Even if you already have a fairly sophisticated security program in place, you will need to document your security assessment and compliance approach in order to ensure compliance with the Security Rule. This will include the development of new, or revisions to existing, policies and procedures.

Compliance Tips

In implementing the Security Rule to bring your organization in compliance by the deadline, keep the following tips in mind to ensure that your policies and procedures thoroughly address the Rule's requirements:

1. Your security assessment should be conducted, and your policies and procedures drafted, with input from the various departments and key constituencies within your organization. While information technology personnel play an important role in some of the more technical controls that may be implemented, it is important to include other individuals (such as administrative, clinical, financial, legal, and risk management personnel) who are attuned to the potential broader operational and legal implications of a particular compliance strategy.

2. "Addressable" specifications cannot be ignored or dismissed summarily. Covered entities must carefully document their decisions to forego adoption of addressable specifications, consistent with the Rule's criteria, as part of their Security Rule assessment process. In the event of a security breach, such "nonadoption" documentation could end up in the hands of government regulators or even opposing counsel, should litigation ensue. Carefully drafted "nonadoption" documentation can go a long way to protect the entity from liability.

3. Although your organization's business associate agreements may comply with HIPAA's Privacy Rule, you should review these agreements to ensure that they incorporate appropriate language to address the Security Rule's business associate requirements. Some business associate arrangements may pose a higher risk of a security breach than others and may warrant negotiation of more explicit and detailed security requirements than the general business associate language contained in the Security Rule.

4. When drafting policies that provide your workforce with the appropriate access to EPHI, be sensitive to the different types of employees and departments in your organization, and link policies and procedures with the results of the risk analysis. Plan time to train employees before the compliance deadline on new policies, procedures, and practices.

5. Recognize that compliance with the Security Rule is not a static exercise. Ongoing evaluations of security controls are necessary to ensure that implemented standards continue to be appropriate and reasonable in light of developing technology.

6. Smaller organizations may wish to join forces and jointly engage technical or legal consultants (or obtain other resources) to assist them with their Security Rule implementation. This might include working through the organizations' trade associations.

This Advisory highlights only some aspects of Security Rule compliance. If you have questions about the Security Rule's requirements generally, or need help ensuring your risk assessment, "nonadoption" documentation, or policies and procedures satisfy legal requirements and appropriately address your organization's risk management issues, please contact one of the following attorneys:

Michelle Wilcox DeBarge
860.297.3702 / mdebarge@wiggin.com

Alyssa B. Moss
860.297.3723 / amoss@wiggin.com.

Other helpful resources may be obtained on our HIPAA web page at www.HIPAA-law.info.

One Century Tower
P.O. Box 1832
New Haven CT
06508-1832
Telephone 203.498.4400
Telefax 203.782.2889

400 Atlantic Street
P.O. Box 110325
Stamford CT
06911-0325
Telephone 203.363.7600
Telefax 203.363.7676

450 Lexington Avenue
Suite 3800
New York NY
10017-3913
Telephone 212.490.1700
Telefax 212.490.0536

One CityPlace
185 Asylum Street
Hartford CT
06103-3402
Telephone 860.297.3700
Telefax 860.525.9380

Quaker Park
1001 Hector Street, Ste. 240
Conshohocken PA
19428-2395
Telephone 610.834.2400
Telefax 610.834.3055

www.wiggin.com