

HEALTH CARE BULLETIN

A Publication of J.H. Cohn LLP

Electronic Records and Patient Privacy Risk Analysis is Key to Compliance with HIPAA Security Rule

Few laws have had as dramatic an impact on the health care industry as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). By now, most health care providers, health plans and other covered entities are intimately familiar with HIPAA's Privacy Rule, which requires you to safeguard and limit disclosure of patients' protected health information ("PHI"). And when you transmit PHI electronically to health plans, clearing-houses, billing services or other partners, you must comply with HIPAA's Electronic Transactions and Code Sets Rule.

Soon a new rule - the Security Rule - will join the HIPAA arsenal. Covered entities must be in compliance with the Security Rule by April 20, 2005 (April 20, 2006, for "small health plans"). Unlike the Privacy Rule, which applies to PHI in all of its forms, the Security Rule is limited to electronic PHI ("E PHI"). How much (or how little) you need to do to comply with the rule depends on the level of risk that your electronic data could be compromised.

Limiting Access to Electronic PHI

Technological developments, like electronic medical records, the Internet, and electronic data interchange ("EDI"), have revolutionized the practice of medicine. They enhance the quality of care by giving physicians access to patients' medical records from virtually anywhere. And they streamline the reimbursement process by allowing health care providers to process claims electronically. Unfortunately, that same technology also

makes it easier for unauthorized persons to intercept sensitive patient information.

The Security Rule, therefore, is a critical counterpart to the Privacy Rule. The Privacy Rule spells out who may have access to PHI, while the Security Rule prescribes standards for ensuring that EPHI is accessible only to those who are authorized to see it.

If you've complied with the Privacy Rule, you may already have made some progress toward compliance with the Security Rule. The Privacy Rule contains a security component, requiring entities to implement appropriate "administrative, physical, and technical safeguards" to protect PHI. The Security Rule provides a more comprehensive and detailed set of security standards for EPHI.

Raising the Standards

The Security Rule covers three areas:

- Administrative safeguards, such as security awareness and training, workforce security, and backup procedures
- Physical safeguards, such as controlling access to your facilities or to individual workstations, and
- Technical safeguards, such as user identification, encryption, automatic logoff and other access controls

In each area, the rule specifies standards (what must be done) and implementation specifications (how to do

Healthcare Services Group

Sam Garruto,
Partner-In-Charge

John Alfonso

Michael Berne

Joseph Cascino

Kevin Clancy

Christopher Ivans

Howard Konicov

James Ledwith

William Lewis

Pete Manzetti

Giorgio Ramacciotti

John Reinhardt

Carol Rizzolo

Mark Spelker

Melody Thornton

Marshall Varano

it). Implementation specifications are classified as required or addressable. But addressable doesn't mean optional. The rule's authors recognized that a security problem may have many alternative solutions, so they built in some flexibility.

For each addressable specification, you need to determine whether the specification is reasonable and appropriate for your organization. If it is, you must implement it. If it isn't, you can either (1) adopt an alternative solution that meets the standard, or (2) elect not to imple-

Five Steps to Compliance with HIPAA's Security Rule

- ***Assess current security, risks, and gaps***
 - ***Develop an implementation plan***
 - ***Implement solution***
 - ***Document Decisions***
 - ***Reassess periodically***
-

ment the specification, if there's no reasonable and appropriate solution and you can meet the standard without it. In either case, you should carefully document the rationale supporting your decision.

Take access control, for example. The standard requires you to have policies and procedures for restricting access to authorized users. Required implementation specifications include unique user IDs and emergency access procedures. Addressable specifications include automatic logoff and encryption/decryption.

Encryption may not be necessary in a small practice that doesn't send protected information to patients via e-mail. But in a larger practice that relies heavily on electronic communications with patients, encryption may be appropriate. The problem, of course, is that patients will need special software to decipher the messages. But alternative technologies - such as secure Web portals or virtual private networks ("VPNs") may overcome this problem.

The rules give you the flexibility to design a solution that's right for your organization.

Assessing Your Risk

Protecting the security of electronic information is a lot like preventing disease. You can't devise an appropriate disease

prevention strategy until you understand the patient's risks. You wouldn't prescribe antimalarial drugs, for example, to patients in the United States or other low-risk areas. But if a patient is planning a trip to the Brazilian Rainforest, it's a different story.

The Security Rule's authors recognized that the level of security required of an entity depends on its risks as well as its resources. Indeed, a risk analysis is one of the required implementation specifications. The Centers for Medicare & Medicaid Services ("CMS") recently published the first in a series of papers providing guidance on the Security Rule, entitled "Security 101 for Covered Entities." In it, the CMS advises covered entities to "balance the risks of inappropriate use or disclosure of EPHI against the impact of various protective measures. This means smaller and less sophisticated practices may not be able to implement security in the same manner and at the same cost as large, complex entities."

Complying with the Security Rule doesn't have to break the bank. The key to cost-effective compliance is to conduct a thorough and comprehensive risk analysis and develop reasonable solutions that reflect your organization's risks and resources.

For more information on the issues discussed in this publication, please contact Sam Garruto, Partner-in-Charge, Healthcare Services Group at sgarruto@jhcohn.com or call 888-JHCOHN-1.

Source: Centers for Medicare & Medicaid Services

The Healthcare Bulletin is published by J.H. Cohn LLP for the general information of its clients, friends and business associates and should not be acted on without prior professional consultation.