"TIPS" from Edie Ruark Dahlhauser

International Center for Chiropractic Office Managers
www.ICCOM.org

HHS Publishes HITECH Breach Notification Interim Final Rule

On August 24th, 2009 we finally saw the publication of interim final regulations implementing the security breach notification provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH").

While the regulations appear to parallel the statutory provisions of HITECH, the process covered entities must follow before notifying a patient of certain breaches of their protected health information (PHI) is not as strict as initially feared. For instance, under the new regulations, covered entities will still engage in a very subjective and fact specific risk assessment before determining when to notify a patient of a breach. The regulations also provide guidance to covered entities and their business associates (BAs) relative to their mutual obligations under the new rules.

Summarized below are some key points and issues we perceive to be relevant to covered entities and business associates under the new regulations.

The breach rules only apply to "unsecured" PHI.

Unsecured PHI is defined as PHI that has not been secured through the use of a technology or methodology specified by HHS. According to HHS guidance released in April 2009, encryption and destruction are the only two ways to secure PHI and avoid breach notification under the Act.

Use the links below to go to HHS' April 2009 "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements".

Fact specific risk assessment.

The Regulations define a "breach" as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy and Security Rules that "compromises the security or privacy" of the PHI." A use or disclosure compromises privacy or security only if it creates "a significant risk or harm to the individual as a result of the impermissible use or disclosure." The regulations identify a number of factors covered entities or business associates may consider during this assessment, including:

1. who impermissibly used or to whom the information was impermissibly disclosed;

2. steps taken to mitigate an impermissible use or disclosure (i.e. lost or stolen laptop is returned and forensic analysis reveals that its information was not opened, altered, transferred or otherwise compromised);

the type and amount of PHI involved.

In the event a notification is deemed necessary based on the facts all notification to individuals and HHS and must be given without "unreasonable delay," but no later than 60 days after discovery."

Exceptions to Breach Rule.

There are also key exceptions relative to the breach rule in situations where there is:

1. an unintentional acquisition, access or use of PHI;

2. inadvertent disclosure; or

disclosure of PHI to person not reasonably able to retain such information.

Business Associates.

Under the new regulations, BAs must comply with the privacy and security regulations, just like covered entities. BAs must have policies and procedures documenting compliance with the privacy rule's use and disclosure provisions and the security rule's administrative, physical and technical safeguards requirements.

An interesting issue is raised relative to when BAs acting as "agents" of a covered entity versus BAs acting as "independent contractors" and the breach notification time frames requirements under both scenarios. If a business associate is acting as an agent of a covered entity then the business associate's discovery of the breach will be imputed to the covered entity. Accordingly, the covered entity will have to provide notifications to the patient and HHS based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity. Conversely, if the business associate is an independent contractor of the covered entity (i.e., not an agent), then the covered entity must provide notification based on the time the business associate notifies the covered entity of the breach.

Among other issues, BA agreements may need to be amended to:

1. clearly address the agent versus independent contractor status of the BA; and

the timing of BA notification to a covered entity following a breach.

Grace Period, Enforcement and Penalties.

Finally, the regulations account for a grace period allowance before HHS expects to begin enforcement. The regulations took effect on September 23, 2009, but HHS has delayed seeking sanctions until February 22, 2010.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

My Summary:

Have your HIPAA Privacy and HIPAA Security policies and procedures in place as written in your manuals. You should have two written sets of policies and procedures. One covering HIPAA Privacy and one covering HIPAA Security. Document your compliance. www.ICCOM.org has manuals available for your compliance.

Talk with your software vendor and make sure that all PHI and EPHI are encrypted. This includes anything you have in any other software program, such as, narrative reports in Microsoft Word.

Make sure that when you get new computers, the old hard drives are destroyed. You cannot just erase them.

Get a copy of all Business Associates Notices of how they protect PHI they receive from you.

If there is a breach of unprotected PHI, report it online to HHS. (the information in the first link above).

Keep in touch with any questions....

Edie Ruark Dahlhauser
President, ICCOM
edie@ICCOM.org
www.ICCOM.org
313.330.0199