EXPERT UPDATE

HIPAA Privacy and Security HHS Issues its Final Rule

HENDERSON BROTHERS

HIPAA Privacy and Security HHS Issues its Final Rule

On January 25, 2013, HHS issued amendments to the HIPAA Privacy Rule, Security Rule and the Breach Notification rule.

There are four final rules that have been combined into one final rule that adopts much of the previously proposed regulations with some clarification and modifications. This document is a brief summary of the final regulations.

Business Associates

Business associates of covered entities are directly liable for compliance with certain HIPAA Privacy and Security Rules' requirements. Section 13401 of HITECH provides that the Security Rule's administrative, physical and technical safeguards, as well as the rule's policies and procedures and documentation requirements, apply to business associates in the same manner as these requirements apply to covered entities and that business associates are civilly and criminally liable for violations of these provisions.

The final rule also broadens the definition of business associate to include -

1) A Health Information Organization, E-prescribing Gateway and any other person or entity that provides data transmission services with respect to PHI to a covered entity and that requires routine access to the PHI; and

2) A person who offers a personal health record to one or more individuals on behalf of a covered entity.

A business associate now includes a "subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." Covered entities must make certain that their business associates are compliant, business associates must make certain their subcontractors are compliant, and so on.

Covered entities and business associates will be liable for the acts of their business associate agents in accordance with the Federal common law of agency, regardless of whether the covered entity has a compliant business associate agreement in place.

Privacy Notices

The final rule requires covered entities to alter their privacy notices to include additional statements regarding the use and disclosure of PHI. The privacy notice will also need to include a statement explaining that individuals can restrict disclosure of PHI to a health plan if the disclosure is for the payment of health care operations and it involves a health care service or item for which the participant has paid out of pocket in full. The new notice will also need to identify that individuals have a right to be notified following a breach.

Breach Notification

The final rule also replaces the breach notification rule's "harm" threshold with a more objective standard. A breach is now defined as the "acquisition, access, use or disclosure" of PHI in a manner not permitted under the privacy rule, which "compromises the security or privacy" of the PHI. The final regulations now require a four-part risk assessment, which is intended to focus more objectively on the risk that PHI has been compromised.

A covered entity or business associate must presume that an acquisition, access, use, or disclosure of PHI in violation of the privacy rule is a breach. This presumption holds unless the covered entity or business associate demonstrates that there is a "low

probability" that the PHI has been compromised based on a risk assessment which considers at least the following factors:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the PHI or to whom the disclosure was made;

(3) Whether the PHI was actually acquired or viewed; and

(4) The extent to which the risk to the PHI has been mitigated. The final rule deletes a narrow exception to the breach definition, which had been included in the 2009 interim regulations, for certain limited data sets if they also exclude dates of birth and zip codes.

HHS has provided clarification in an unofficial document that a reportable breach may occur even though the covered entity itself has not violated the privacy rule. If a third party commits a crime, such as theft of a covered entity's PHI, there is an unauthorized disclosure of the PHI. If all of the other requirements for a reportable breach are present, the covered entity must report the breach.

GINA

The final regulations modify the HIPAA Privacy Rule, as required by GINA. HIPAA prohibits most health plans from using or disclosing genetic information for underwriting purposes.

Compliance Date

Although the final regulations are to go into effect on March 26, 2013, compliance is not required until September 23, 2013. This six month period gives covered entities and business associates time to amend agreements and modify policy and procedures.

Final Regulations –
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Contributor:

Shari Herrle
Henderson Brothers, Inc.
Director of Compliance

Please note that the information contained in this document is designed to provide authoritative and accurate information, in regard to the subject matter covered. However, it is not provided as legal or tax advice and no representation is made as to the sufficiency for your specific company's needs. This document should be reviewed by your legal counsel or tax consultant before use.

EXPECT AN EXPERT