HITECH Frequently Asked Privacy, Security Questions: part 2

By Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA, and Adam H. Greene, JD, MPH

Editor's note: This is the second installment of a three-part series reviewing AHIMA's HITECH frequently asked questions.

The final HITECH-HIPAA Omnibus Rule was released in January 2013 and expanded some of HIPAA's original requirements involving its privacy, security, and enforcement components. The Omnibus also finalized the Breach Interim Final Rule as well as the Genetic Information Nondiscrimination Act (GINA).

The following are some commonly asked questions about the HITECH Omnibus Rule implementation and compliance requirements, specifically regarding the rule's areas addressing business associates, breaches, and GINA.

Business Associates and Subcontractors

The final rule changed the definition of business associate to essentially any organization that creates, receives, maintains, or transmits personal health information (PHI) for a function or activity on behalf of the covered entity. The full definition can be found in subparts A and B of Part 160 of HIPAA or 78FR5570 of the final rule.

The HITECH Act explicitly made business associates liable for noncompliance for specific requirements of the HIPAA Privacy Rule. The Privacy Rule does not create direct liability for business associates with regard to compliance with all requirements under the Privacy Rule. A business associate is directly liable under the Privacy Rule for uses and disclosures of PHI that are not in accord with its business associate agreement or the rule.[1] The Omnibus Rule also added a statement that the Security Rule now applies to business associates as well.

Business Associate FAQs

Q: By what date must business associate agreements be updated?

A: If you have a HIPAA-compliant agreement in place prior to January 25, 2013, and if it was not due to be renewed by September 23, 2013, then the parties have until September 23, 2014 to revise the agreement. In contrast, if the covered entity or business associate first executes a business associate agreement on or after January 25, 2013, or had an agreement in place as of January 25, 2013 but modified it on or after March 26, 2013, then the parties must either ensure that the new agreement or modifications comply with the new rule or must have revised the agreement no later than September 23, 2013 to bring the agreement into compliance with the new rule.

If an agreement is renewed between September 23, 2013 and September 23, 2014, it must comply with the new Omnibus Rule.

Q: Do you need a business associate agreement for a hospital's foundation?

A: A covered entity may use or disclose to a business associate or to an institutionally related foundation the following protected health information for the purpose of raising funds for its own benefit without an authorization meeting the requirements of HIPAA §164.508:

- Demographic information relating to an individual, including their name, address, other contact information, age, gender, and date of birth

- Dates of healthcare provided to an individual
- Department of service information
- Treating physician
- Outcome information and health insurance status

A covered entity must include the required statement for fundraising in its Notice of Privacy Practices stating that protected health information (PHI) may be used for fundraising and that the individual may opt out.

Q: If the hospital has a business associate agreement with a company and that company subcontracts, does the hospital need to have a copy of the subcontractor's business associate agreement on file?

A: No. The final rule expressly provides that a covered entity is not required to enter into a business associate agreement with a business associate that is a subcontractor. Rather, this is the obligation of the business associate that has engaged the subcontractor to perform a function or service that involves the use or disclosure of PHI.

Q: Are business associates only responsible for reporting breaches to the covered entities they perform services to, or must they also report to the Department of Health and Human Services (HHS)?

A: According to the rule, a subcontractor reports the breach to the business associate, the business associate reports the breach to the covered entity and the covered entity reports the breach to the affected individuals, the Department of Health and Human Services, and, if applicable, the media, unless it has delegated such responsibilities to a business associate.

Breaches and Breach Notification

The final Omnibus Rule adopted the Breach Interim Final Rule into law, with some changes. Definition of a breach was changed. The Office for Civil Rights (OCR) added language to the definition of a breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Also, harm threshold was replaced with a breach risk assessment. Therefore instead of assessing the risk of harm to the individual, covered entities and business associates must assess the probability that the PHI has been compromised based on a risk assessment. Risk assessments should be objective in nature.

Breach FAQs

Q: Protected health information was faxed to the wrong nursing home. The recipient of the fax was a covered entity. Is this a breach?

A: In this case the recipient has obligations to protect the privacy and security of the disclosed information. There may be a reasonable basis to conclude that this was not a breach after documenting a breach risk assessment that includes at least four factors set forth in the Breach Notification Rule, including the identity of the unauthorized recipient. The fact that the unauthorized recipient is subject to HIPAA will substantially lower the risk of compromise, but the covered entity should still address all four factors.

Q: What should I do if information is breached during a disaster?

A: A disaster likely represents "reasonable delay" with respect to making required breach notifications. If breach notifications cannot be made within 60 days, however, it may be helpful to contact the regional OCR to inquire about whether they will exercise enforcement discretion and provide additional notification time.

Genetic Information Nondiscrimination Act (GINA)

The Omnibus Rule adopts the proposed GINA rule and applies a prohibition on using or disclosing genetic PHI for underwriting purposes to all health plans that are covered entities under the HIPAA Privacy Rule, including those to which

GINA does not expressly apply, except with regard to issuers of long-term care policies. HIPAA expands the prohibition on underwriting with genetic information from the four types of entities expressly listed in GINA (group health plans, health insurance issuers, health maintenance organizations, and issuers of Medicare supplemental policies) which includes employee welfare benefit plans, high-risk pools, certain public benefit programs, and any other individual or group plan or combination of individual or group plans. At this time issuers of long-term care policies are exempted.

GINA FAQs

Q: Is it a regulation violation if a health insurance company offering an employer-sponsored group health plan uses an individual's family medical history or genetic test results, maintained in the group health plan's claims experience information, to adjust the plan's blended, aggregate premium rate for the upcoming year?

A: Yes. The issuer would be using protected health information—genetic information—for underwriting purposes, which is a violation of federal regulation 45 CFR 164.502(1)(5)(i).

Q: A group health plan uses family medical history information provided by an individual, incidental to the collection of other information on a health risk assessment, to grant a premium reduction to the individual. Is this a violation?

A: Yes, the group health plan would be using genetic information for underwriting purposes, which is a violation of federal regulation 164.502 (1)(5)(i).

Note

1. AHIMA. "Analysis of Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rule." January 25, 2013.

Angela Dinh Rose (angela.rose@ahima.org) is a director of HIM practice excellence at AHIMA. Adam H. Greene (adamgreene@dwt.com) is a partner at Davis Wright Tremaine LLP, based in Washington, DC.

Article citation:
Rose, Angela Dinh; Greene, Adam H. "HITECH Frequently Asked Privacy, Security Questions: part 2" *Journal of AHIMA* 85, no.2 (February 2014): 48-49.