At-a-Glance:
Amendments to the Health and Information Portability and Accountability Act (HIPAA)
Under the American Reinvestment and Recovery Act (ARRA) of 2009

Introduction

When the American Reinvestment and Recovery Act of 2009 was passed, it amended certain portions of HIPAA to bring the Act up to date as well as expanding its scope. These amendments became effective and enforceable in 2010 with the passage of the HIPAA Omnibus Final Rule.[1] Primarily, the Enforcement, Security, Privacy, and Breach Notification Rules were amended so that their provisions would apply to Business Associates in certain respects. Additionally, HIPAA was amended to bring the Act in compliance with the more-recently enacted provisions of the Genetic Information Nondiscrimination Act (GINA) of 2008 as well as the Patient Safety and Quality Improvement Act (PSQIA) of 2005. Each amended portion of HIPAA is detailed below.

I. Business Associates

HIPAA now requires that covered entities enter into contracts with their business associates to ensure that any Protected Health Information (PHI) that the business associate receives or maintains on behalf of the covered entity is adequately secured. This requirement also extends to subcontractors of business associates that create, receive, maintain, or transmit PHI on behalf of the business associate. Additionally, the ARRA amendments expand the definition of business associate to include health exchange organizations, e-prescribing gateways, and regional health information organizations which transmit PHI to a covered entity or a business associate and which is also routinely accessing the PHI. Also, if a vendor contracts with a covered entity to offer PHI to patients as a part of the covered entity's electronic health record (EHR), that vendor is considered a business associate. The amendments to the Enforcement, Security, and Privacy Rules also affect covered entity's relationships with business associates. Each of these changes is detailed in the corresponding sections that follow.

II. Enforcement Rule

The HIPAA Enforcement Rule has been reworked in a number of notable ways. The Enforcement Rule now operates within a 4-tier violation framework that is stricter than the previous Enforcement Rule. Additionally, business associates of covered entities can be directly liable for civil monetary penalties that accrue as a result of HIPAA violations. The new tiered violation framework is as follows:

- Tier 1 violation: unknowing violation where the covered entity or business associate did not know about the violation and could not have known about it through the exercise of reasonable diligence – $100-$50,000 per violation.
- Tier 2 violation: the covered entity or business associate either knew of, or could have discovered the violation through the exercise of reasonable diligence – $1,000-$50,000 per violation.
- Tier 3 violation: the violation was the result of willful neglect, but was corrected within 30 days of being discovered – $10,000-$50,000 per violation.
- Tier 4 violation: the violation was the result of willful neglect but was not corrected within 30 days – at least $50,000 per violation.

The amount of each violation will be determined on a case-by-case basis by the Secretary of the Department of Health and Human Services – Office for Civil Rights (OCR). The 30-day cure period begins on the date that the covered entity or business associate obtains actual or constructive knowledge of the violation, and the yearly cap for all identical violations committed by the same entity is set at $1.5 million.

The Secretary must formally investigate complaints of HIPAA violations due to willful neglect, and the Secretary has been given the discretion to determine the amount of the civil monetary penalty that he or she levies based on the extent of the harm caused by the violation. A civil monetary penalty *must* be issued against the

[1] This can be found at: [https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-122].

offending covered entity or business associate, except in the case where the violation is not caused by willful neglect and the Secretary chooses to waive the penalty. The following factors will be considered by the Secretary when determining the amount of the civil monetary penalty: the nature of the claims and circumstances surrounding the violation, the history of prior offenses and financial condition of the person presenting the claims, as well as the covered entity or business associate's previous history of HIPAA compliance. The Secretary is also charged with conducting compliance reviews of covered entities and business associates to determine if HIPAA violations are being caused by the willful neglect. To ensure that the Secretary's investigations do not cause the security of PHI to be compromised, the Enforcement Rule has been amended with strict safeguards concerning how the relevant PHI is handled.

Before the ARRA amendments, there was an affirmative defense against the imposition of civil monetary penalties if the covered entity did not know of the violation and could not have discovered it through the exercise of reasonable diligence. This affirmative defense has been removed, and instead this sort of violation is punishable under the lowest tier of violations under the 4-tier framework.

III. Security Rule

The amendments to the Security Rule under ARRA, like the other portions of the amendments, expand the operation of the Rule to include business associates. Specifically, the Security Rule's technical safeguard requirements of §164.308, §164.310, and §164.312, as well as the Security Rule's procedural and administrative requirements of §164.316 have been expanded to apply to business associates in the same manner that they apply to covered entities. The amended Security Rule makes it clear that business associates can be civilly and criminally liable for violations of these provisions. Additionally, under the amended §164.306, both covered entities and business associates are charged with periodically monitoring and reviewing their security measures to ensure compliance with HIPAA as well as the reasonable and appropriate protection of PHI.

The Security Rule has been amended so that the termination procedures for workforce members also include volunteers, not just employees. Also, covered entities may now permit business associates to create, receive, maintain, or transmit PHI as long as there is a contract or a similar arrangement in place to guarantee that the business associate will adequately safeguard the PHI. These business associate agreements must conform with §164.308(b). The remaining amendments to the Security Rule were technical changes that were made to implement these new standards.

IV. Privacy Rule

The HIPAA Privacy Rule has been amended to bring it in compliance with the Patient Safety and Quality Improvement Act of 2005. This categorizes patient safety organizations (PSOs) as business associates of covered health care providers, and patient safety operations by PSOs of covered health care providers as health care operations under the new Privacy Rule. Additionally, the Privacy Rule has been amended to expand the types of rights that patients have concerning the use of their PHI and how they are contacted for marketing communications.

Covered entities and business associates will be required to get an authorization from the patient for all treatment and health care operation communications where the covered entity receives remuneration from a third party for making the communication. Such authorizations are required for all subsidized communications that market a health-related product or service, and these are all considered marketing communications under the new Privacy Rule. This authorization requirement also extends to business associates and subcontractors. The patient can revoke their authorization at any time to stop receiving the marketing materials. For a business associate's use of PHI to be permissible, it must comply with the business associate contract and the "minimum necessary" standard of the Privacy Rule. §164.502(b) defines the "minimum necessary" standard, and requires that when a business associate uses, discloses, or requests PHI from a covered entity, they must limit the PHI used to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request. Additionally, the business associate contract must contain "satisfactory assurances" that the business associate will appropriately safeguard the PHI in accordance with §164.502(e) and §164.504(e).[2] There are seven exceptions to the authorization requirement where a business associate contract is not required. An authorization is not required where the purpose of the exchange is for: 1) public health activities; 2) research purposes; 3) the treatment of the individual; 4) the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence; 5) services

[2] Sample business associate agreements are available on the Department of Health and Human Services website at: [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html].

rendered by a business associate pursuant to a business associate agreement, and at the specific request of the covered entity; 6) providing an individual with access to their PHI; and 7) other purposes left to the Secretary of OCR.

Patients have the right to request a restriction of uses and disclosures under §164.552(a). Covered entities are required to permit individuals to request that they restrict uses or disclosures of their PHI for treatment, payment, healthcare operations, and disclosures to family members. Covered entities are not required to agree to such a request, but if they do then they are bound by that decision going forward, except in the situation where the information is required to be disclosed to treat the patient in emergency circumstances. Covered entities are required to agree to the nondisclosure request if the restriction is on the disclosure of PHI to a health plan for carrying out payment or health care operations or if the patient has paid the health care provider in full and out of pocket. The individual has a right to determine which health care items or services that they wish to be paid for out of pocket, which will sometimes require that services be unbundled and itemized.

Patients also have the right to review or obtain copies of their PHI to the extent that it is maintained by the covered entity. Where the covered entity maintains PHI in an electronic format, the individual has a right to request it in the same format. If there are complications, a hard copy will suffice. The covered entity may impose a fee for providing a copy of the PHI, but this fee can only include: 1) the cost of supplies and labor for copying the PHI; 2) the cost of postage, if applicable; and 3) the cost of preparing an explanation or summary of the information. The cost of labor and portable media to store the PHI on can also be included in this fee. If the request is approved, the PHI must be provided within 30 days of its approval.

V. Breach Notification Rule

The Breach Notification Rule has been amended to provide for stricter notification measures in the result of a breach. A "breach" is any unauthorized acquisition, access, use, or disclosure of PHI which compromises its security or privacy. There are three exceptions to this: 1) the unintentional acquisition, access, or use of PHI by an employee or a business associate of the covered entity if the access was made in good faith and within that person's scope of employment, and the PHI is not further disclosed or compromised; 2) inadvertent disclosure of PHI from an authorized person at a facility operated by the covered entity, and the PHI is not further disclosed or compromised; and 3) unauthorized disclosures in which the unauthorized person would not reasonably have been able to retain the information. In the event of a breach, covered entities must provide notification to the affected individuals and the Secretary of OCR when the breach is discovered. If a business associate commits a breach, it must instead notify the covered entity. HHS will publish a list online of all breaches of unsecured PHI that involve the information of 500 or more people. The Secretary of OCR can be notified of a breach here: [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html].

VI. Genetic Information Nondiscrimination Act

There are two substantial changes to HIPAA under GINA, both of which bar discrimination based on the use of a person's genetic information. Title I prohibits discrimination in premiums or contributions for group coverage based on a person's genetic information. It also prohibits the use of genetic information as a basis for determining eligibility or setting premiums in Medicare and Medigap insurance markets. Title I limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing to determine coverage. Title II prohibits employers from using genetic information when making employment decisions. Specifically, employers and other entities covered by this section are restricted from requesting, requiring, or purchasing genetic information and it restricts the ability of those entities from disclosing genetic information. Title I is enforced by the Department of Labor, the Department of the Treasury, and the Department of Health and Human Services, while Title II is enforced by the Equal Employment Opportunity Commission.