Client Advisory

CARTER LEDYARD & MILBURN LLP
Partners for Your Business®

Cybersecurity Practice Group

July 14, 2017

Guidance on Cybersecurity: The HIPAA Breach Notification Rule

Practitioners and servicers in the health care industry rely heavily on electronic storage and transmission of patient health information. As we discussed in our client advisory *Guidance on Cybersecurity: The HIPAA Security Rule*,[1] the health care industry is a prime target for cyber-attacks, and the U.S. Department of Health and Human Services ("HHS") enforces its *Security Standards for the Protection of Electronic Protected Health Information* (the "HIPAA Security Rule" or "Security Rule") to establish industry-wide standards for the protection of patient health information.[2] However, despite companies' best efforts to comply with the HIPAA Security Rule, companies in the health care industry remain at risk of experiencing data breaches that result in unauthorized access to private health information. In the event of a data breach, entities subject to HIPAA must comply with the provisions of the HIPAA Breach Notification Rule (the "HIPAA Notification Rule" or "Breach Notification Rule"), which requires covered entities to notify individuals, the media, and the Secretary of HHS upon detecting a breach of unsecured PHI. Additionally, a business associate must notify a covered entity for whom the business associate is holding data if the business associate discovers a breach of that data.[3]

HHS has recently started focusing on enforcing the HIPAA Notification Rule. Earlier this year, the agency announced its first settlement based on the untimely reporting of a breach of unsecured PHI. The settlement required Presence Health Network to pay $475,000 and enter into a Corrective Action Plan agreement with HHS as a consequence of its delay in notifying individuals (which was delayed by 44 days), the media (by 46 days), and HHS (by 41 days) of a breach of unsecured PHI.[4] Notably, in that case HHS considered each day on which Presence Health Network failed to send a required notice as a separate violation of the Breach Notification Rule.

As a result of HHS's new focus on enforcement, entities that are subject to the Breach Notification Rule should take special care to comply with the administrative requirements of the Rule and to adopt or review procedures to ensure that the appropriate notices are given if there is a breach. In this client advisory, we will

---

[1] *Available at* http://www.clm.com/docs/7915541_4.pdf.
[2] Codified at 45 C.F.R. Part 160 and Subparts A and C of Part 164.
[3] Entities that are not subject to HIPAA, and thus not subject to the HIPAA Notification Rule, such as vendors of personal health records (e.g., websites or apps that allow patients to directly input their health data) and third-party service providers with access to health information, may nonetheless be subject to the Federal Trade Commission's Health Breach Notification Rule, which is codified at 16 C.F.R. Part 318.
[4] *See* HHS, First HIPAA Enforcement Action for Lack of Timely Breach Notification Settles for $475,000 (Jan. 9, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/presence/index.html.

first discuss the relevant administrative requirements of the Security Rule and then discuss the applicability and technical requirements of the Breach Notification Rule.

Administrative Requirements

The HIPAA Security Rule contains several administrative requirements related to promoting compliance with the Breach Notification Rule. The Breach Notification Rule mandates that entities subject to its requirements must also comply with the administrative requirements of the Security Rule. Therefore, failure to comply with those administrative requirements could lead to enforcement consequences with respect to both the Breach Notification Rule and the Security Rule. Companies in the health care industry should consider consulting with counsel to determine the most effective approach to implementing the requirements. Specifically, entities subject to the requirements of the Breach Notification Rule must:

(i) provide workforce and officer training with respect to the Breach Notification Rule;

(ii) provide a process for individuals to make complaints with respect to the covered entity's policies or procedures or its compliance with such policies and procedures;

(iii) apply appropriate sanctions to members of the workforce who do not comply with the Breach Notification Rule;

(iv) refrain from intimidating, threatening, coercing, discriminating against, or taking a retaliatory action against any individual with respect to the individual's participation in any process provided for in the Breach Notification Rule;

(v) not require any individual to waive his or her rights under the Breach Notification Rule (e.g., requiring an individual to allow notice via email) in order to receive treatment, payment, enrollment in a health plan, or eligibility for benefits;

(vi) adopt policies and procedures with respect to the requirements of the Breach Notification Rule, and maintain such written policies and procedures in electronic or written form.[5]

The HIPAA Breach Notification Rule

Background

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS published the HIPAA Security Rule in 2003, which created a national standard of technical and non-technical safeguards to

[5] 45 C.F.R. § 164.414, citing various provisions of the Security Rule codified at 45 C.F.R. § 164.530. For more information about the requirements of the HIPAA Security Rule, see our previous client advisory, *Guidance on Cybersecurity: The HIPAA Security Rule*, available at http://www.clm.com/docs/7915541_4.pdf.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

protect electronic protected health information ("PHI").[6] All "covered entities" and "business associates" are subject to the HIPAA Security Rule.[7] The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which was enacted as part of The American Recovery and Reinvestment Act of 2009,[8] required HHS to adopt a rule requiring covered entities and business associates to notify patients and HHS upon experiencing certain data breaches. Accordingly, HHS promulgated the HIPAA Notification Rule.[9]

Applicability

The HIPAA Notification Rule is applicable only to unsecured PHI. "Unsecured PHI" is PHI that "is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology" specified by HHS.[10] PHI is considered "secured," and thus not subject to the Breach Notification Rule, if it:

(i) is encrypted as specified in the Security Rule, and the confidential process or key that can be used to decrypt the information has not been breached;[11] or

(ii) the media on which the PHI is stored has been destroyed by:

a. shredding or destroying the paper, film, or other hard copy such that it cannot be read or otherwise reconstructed (Redaction is specifically excluded as a means of destroying information.); or

b. clearing, purging, or destroying electronic media pursuant to National Institute of Standards and Technology ("NIST") guidelines.[12]

Although a company may have implemented data security policies or technology in compliance with the Security Rule, it is still subject to the Breach Notification Rule unless the breached data was subject to the

---

[6] "Protected health information" means individually identifiable health information relating to: (1) an individual's physical or mental health condition; (2) the provision of health care to an individual; or (3) payment for the provision of health care to an individual.

[7] A "covered entity" is (1) a health plan, (2) health care clearinghouse, or (3) a health care provider that electronically transmits any health information in connection with administrative or financial transactions regulated by HHS. A "business associate" is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, the covered entity that involve the use or disclosure of individually identifiable health information. Common examples include claims processing, accounting, legal work, consulting, management services, data aggregation, and accreditation services.

[8] Pub. L. 111-5, codified at 16 U.S.C. ch. 46 §2601, et seq., 42 U.S.C. ch. 134 § 13201 et seq., 42 U.S.C. ch. 149 § 15801 et seq.

[9] The text of the HIPAA Notification Rule is codified at 45 C.F.R. §§ 164.400–414.

[10] 45 C.F.R. § 164.400.

[11] *See* NIST Special Publications 800-111, "Guide to Storage Encryption Technologies for End User Devices"; 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TSL) Implementations"; 800-77, "Guide to IPsec VPNs"; 800-113, "Guide to SSL VPNs."

[12] NIST Special Publication 800-88, "Guidelines for Media Sanitization."

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

specific encryption or sanitization measures specified in the applicable NIST guidelines or to equivalent security measures.[13]

What Is A Breach?

A breach is "the acquisition, access, use or disclosure of [PHI] in a manner not permitted under [the Security Rule or the HIPAA Privacy Rule]."[14] The following are exceptions to the definition of a breach:

(i) unintentional acquisition, access or use by members of the workforce or other persons acting under the authority of a covered entity or business associate, so long as the act was in good faith within the scope of authority and does not result in further unpermitted uses or disclosures;

(ii) inadvertent disclosures of one person authorized to access the PHI to another person who is also authorized to access the PHI, so long as the disclosure does not result in further unpermitted uses or disclosures;

(iii) disclosures of PHI where the covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure was made could not reasonably have been able to retain such information.[15]

When data is impermissibly acquired, accessed, used or disclosed, a breach is presumed 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 of at least the following factors":

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

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

(iii) whether PHI was actually acquired or viewed; and

(iv) the extent to which the risk to PHI has been mitigated.[16]

A covered entity or business associate may choose to provide the required notifications without undertaking the risk assessment described above. However, an entity may not choose to forego providing the required notifications without first performing a risk assessment.

---

[13] *See* HHS, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (July 26, 2013), *available at* https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.
[14] 45 C.F.R. 164.402.
[15] *Id.*
[16] *Id.*

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

Notice to Individuals

In general, following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed as a result of the breach. A covered entity is deemed to have discovered a breach if the breach is known, or would have been known through the exercise of reasonable diligence, by any person who is a member of the workforce or agent of the covered entity, other than the person committing the breach.[17]

Notice must be provided "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach."[18] If the covered entity can reasonably give notice prior to 60 days after discovering the breach, then it must do so. However, if a law enforcement official states that "a notification, notice, or posting required under [the Breach Notification Rule] would impede a criminal investigation or cause damage to national security," the notice may be delayed by a period of time as specified by the law enforcement official in a written statement or, if the statement is oral, for no longer than 30 days from the time of the oral statement unless a written statement specifying a longer period is subsequently provided by the law enforcement official.[19]

The notice must include (and may be made in separate notices as information becomes available):

(i) a brief description of what happened, including the date of the breach and the date of discovery, if known;

(ii) a description of the types of PHI that were involved in the breach, such as name, social security number, diagnoses, address, or account number;

(iii) any steps individuals should take to protect themselves from potential harm;

(iv) a brief description of the covered entity's measures to investigate the breach, mitigate harm to individuals, and prevent future breaches; and

(v) contact information for the covered entity, including a toll-free telephone number, email address, website, or mailing address.[20]

The notice must be written in plain language and delivered in written form by first-class mail to each individual's last known address, or to an individual's email address if such individual has agreed to receive notice by email and that agreement has not been withdrawn. If the covered entity knows that an individual is

---

[17] 45 C.F.R. § 164.404(a). The "workforce" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." Whether an individual is an "agent" of a covered entity or business associate is "determined in accordance with the federal common law of agency." *Id.*

[18] *Id.*

[19] 45 C.F.R. § 164.412.

[20] *Id.*

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

deceased and has the address of the next of kin or personal representative of the deceased individual, written notification by first class mail must be provided to either the next of kin or personal representative.[21]

If the covered entity's contact information for any individuals is insufficient or out-of-date, the covered entity must provide substitute notice as follows:

(i) For fewer than 10 individuals, by an alternative form of written notice, telephone notice, or other means.

(ii) For 10 or more individuals, by:

a. a conspicuous notice either on the covered entity's homepage for 90 days, or in major print or broadcast media in the geographic areas where the affected individuals likely reside; and

b. a toll-free phone number that remains active for 90 days, where a person who sees the notices may call to find out if his or her PHI may be included in the breach.[22]

If the covered entity feels that the situation "requires urgency" due to a threat of "imminent misuse" of PHI, it may notify affected individuals by telephone or other means in addition to providing the written notice described above.[23]

Notice to the Media

If a breach of unsecured PHI affects more than 500 residents of a state or jurisdiction, then the covered entity must notify "prominent media outlets" serving that state or jurisdiction. The notice must meet the same requirements as a notice to individuals (discussed above), and it must be made within the same time period (i.e., without unreasonable delay and in no case more than 60 days after discovery of the breach, subject to a law enforcement delay).[24]

Notice to HHS

All breaches of unsecured PHI must be reported to the Secretary of HHS. The covered entity must maintain a log of breaches involving fewer than 500 individuals, and all such breaches for the preceding calendar year must be reported to HHS no later than 60 days following the end of that calendar year (March 1st or February 29th). For breaches involving 500 or more individuals, the covered entity must provide notice to HHS contemporaneously with the notice to individuals, subject to a law enforcement delay, as discussed above.[25]

---

[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] 45 C.F.R. § 164.406.
[25] 45 C.F.R. § 164.408. In both cases, such notice must be made as provided on the HHS website, hhs.gov/hipaa//for-professionals/breach-notification/breach-reporting/index.html.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

Business Associates

A business associate must notify the covered entity following discovery of a breach of unsecured PHI, without unreasonable delay and in no case later than 60 days following discovery. As for covered entities, a breach is deemed to be discovered when it is known, or should have been known through the exercise of reasonable diligence, by an employee, officer, or other agent of the business associate, other than the person committing the breach.[26] The notice must contain, to the extent possible, the identification of each individual affected by, or reasonably believed by the business associate to be affected by, the breach, and any other available information that will be required in the notice to individuals, as discussed above.[27]

Although a covered entity is ultimately responsible for notifying individuals affected by a breach of unsecured PHI, a covered entity may delegate some or all of its duties with respect to such notices to a business associate.[28] However, a covered entity may not delegate its duties with respect to notifying the media or HHS.

Burden of Proof

Each covered entity and business associate has the burden of demonstrating that all required notifications were made or that a use or disclosure does not constitute a breach.[29]

Conclusion

Although companies in the health care industry continue to adopt and improve cyber security measures, some will inevitably experience breaches of PHI by cyber attackers or even by employees, officers, or agents. If and when a breach occurs, it is critical that the affected covered entity or business associate notify the individuals and entities that it is required to notify pursuant to the Breach Notification Rule. HHS has recently stepped up enforcement of the Breach Notification Rule, and failure to comply with the Rule could lead to costly penalties. Thus, companies should prioritize the adoption of policies and procedures that will help ensure compliance with the Breach Notification Rule.

For more information concerning the matters discussed in this publication, please contact the authors **Michael H. Bauscher** (212-238-8785, bauscher@clm.com) or **Kortni M. Hadley** (212-238-8871; hadley@clm.com), or your regular Carter Ledyard attorney.

---

[26] Discovery of a breach by a business associate is limited to breaches known to officers and employees, unlike discoveries by covered entities, which include breaches known to unpaid volunteers or trainees. As with agents of covered entities, agents of business associates are determined in accordance with the federal common law of agency. 45 C.F.R. § 164.410.
[27] 45 C.F.R. § 164.410.
[28] 45 C.F.R. § 164.404.
[29] 45 C.F.R. § 164.414.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232