11 February 2016

Practice Groups:

Cyber Law and Cybersecurity;

Global Government Solutions;

Government Enforcement;

Health Care

Government Investigations Into Cybersecurity Breaches In Healthcare

By: Mark A. Rush, Patricia C. Shea, Eric M. Matava

In September 2015, a U.S. Department of Health and Human Services (HHS), Office of the Inspector General (OIG), report found that the Office of Civil Rights (OCR), the agency charged with ensuring compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), had not "fully implemented the required audit program to proactively assess possible noncompliance from covered entities."[1] The HHS OIG report described OCR's oversight as "primarily reactive."[2] As a result, the report recommended the implementation of a permanent audit program, scheduled to begin in early 2016.[3] This development poses risks to healthcare providers faced with cybersecurity breaches and the potential for government investigations into the steps taken to address them.

In order to minimize exposure and prepare for any subsequent government investigation, healthcare providers must ensure that they have implemented the safeguards HIPAA requires. In the event these safeguards are unsuccessful in preventing a breach, healthcare providers must have an effective incident response plan in place. This article reviews the reporting obligations under HIPAA, provides an overview of state notification laws that may supplement HIPAA, reviews the potential consequences associated with noncompliance, and highlights several key steps for responding to a data breach.

Background

HIPAA's Privacy Rule protects health information about individuals regarding their past, present, or future physical or mental health condition; the care provided to them; and the past, present, or future payment for the care. When this information is created or received by a healthcare provider, health plan, or healthcare clearinghouse, HIPAA terms it "Protected Health Information" or "PHI."

A breach of unsecured PHI is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted by [the Privacy Rule] which compromises the security or privacy of the protected health information."[4] Most breaches that healthcare providers encounter fall into one of the following categories: lost or stolen electronic devices, hacking, employee misconduct, improper disposal, unauthorized training, and unsecured records. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity is able to demonstrate that there is a low probability that PHI has been, or will be, compromised.[5] The regulations do not define "compromise." Instead, the regulations require healthcare

---

[1] U.S. Department of Health and Human Services, Office of Inspector General, *OEI-09-10-00510: OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards* 2 (2015).

[2] *Id.*

[3] Greg Slabodkin, *McGraw Discusses HIPAA Audits Slated for Early 2016*, HEALTH DATA MANAGEMENT (Oct. 22, 2015, 2:53pm), http://www.healthdatamanagement.com/news/OCR-Provides-Details-on-HIPAA-Audits-in-Early-2016-51441-1.html.

[4] 45 C.F.R. § 164.402. *See* 45 C.F.R. § 164.402(1) (i–iii), for certain limited exclusions to the definition of "breach."

[5] 45 C.F.R. § 164.402(2).

providers and other entities subject to HIPAA (collectively, "covered entities") to conduct a risk assessment of at least the following factors:

(1) The type and amount of PHI involved;

(2) Who impermissibly used the PHI or to whom was the PHI impermissibly disclosed;

(3) The extent to which the risk to the PHI has been mitigated; and

(4) Whether the PHI was actually acquired or viewed.[6]

Covered entities must document their risk assessments in order to demonstrate, if necessary, that no breach notification was required.[7] The burden of proving that notification was not required rests with covered entities, and this documentation is a key component in satisfying this burden.

Complying With the Breach Notification Rule

HIPAA's Breach Notification Rule requires covered entities to notify certain individuals and entities once a breach of *unsecured PHI* has occurred.[8] Unsecured PHI is defined as PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology" specified by the secretary of HHS in guidance.[9] According to HHS, unsecured PHI is PHI that has neither been encrypted nor properly destroyed.[10] As noted above, not all unauthorized acquisition, access, use, or disclosures of PHI necessarily amounts to a breach, but if it does and the information is unsecured, a covered entity must notify the affected individuals, the secretary of HHS, and, in some cases, prominent media outlets.[11] The covered entity must notify the respective parties without unreasonable delay, but under no circumstances later than 60 days from the date of discovery of the breach.[12] A breach is discovered by a covered entity as of the first day on which the breach is known to the covered entity, or, would have been known to the covered entity with the exercise of reasonable diligence.[13]

Notice to Affected Individuals: Notice should be provided in writing by first-class mail to the individual at his or her last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.[14] If there is insufficient or out-of-date contact information that precludes written notification to the individual, the reporting entity may use a substitute form of notice reasonably calculated to reach the individual instead.[15]

Notice to the Secretary of HHS: In any case in which a breach is reportable, the covered entity

[6] 45 C.F.R. § 164.402(2)(i–iv).

[7] 78 Fed. Reg. 5577, 5644 (Jan. 25, 2013).

[8] 45 C.F.R. § 164.404(a)(1).

[9] 45 C.F.R. § 164.402.

[10] U.S. DEPT. OF HEALTH AND HUMAN SERVICES, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

[11] 45 C.F.R. § 164.404–408.

[12] 45 C.F.R. § 164.404(b).

[13] 45 C.F.R. § 164.404(a)(2).

[14] 45 C.F.R. § 164.404(d).

[15] *Id.* The specific form of alternative notice depends on the amount of individuals for whom there is insufficient contact information.

must notify the secretary of HHS.[16] However, the time at which this notification must be provided depends on the number of individuals affected by the breach.[17]

If fewer than 500 individuals are involved in a particular incident, the covered entity must notify the secretary within 60 days after the end of a calendar year of any and all breaches of this type that occurred during the previous calendar year, although the covered entity may elect to notify the Secretary sooner.[18] If more than 500 individuals are involved in any particular incident, the covered entity must notify the secretary concurrently with the notice it provides to the affected individuals.[19]

Notice to the Media: In cases involving more than 500 individuals within a state or jurisdiction, HIPAA requires that notice be provided to prominent media outlets serving that particular state or jurisdiction.[20]

Elements of Notification: The notice must include the following elements, to the extent applicable:

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

(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, or postal address.[21]

The notice must also be written in plain language and must be in writing, except in certain circumstances where substitute notice is permitted because the contact information for individuals is unknown.[22]

State Breach Notification Statutes

As of January 1, 2016, 47 states have passed their own breach notification laws.[23] The requirements in each state's law will be preempted by any contrary provisions in HIPAA or any of its applicable implementing regulations, unless the state law is considered more stringent than

[16] 45 C.F.R. § 164.408(a).
[17] 45 C.F.R. § 164.408(b–c).
[18] 45 C.F.R. § 164.408(c).
[19] 45 C.F.R. § 164.408(b).
[20] 45 C.F.R. § 164.406(a).
[21] 45 C.F.R. § 164.404(c)(1) (A–E).
[22] 45 C.F.R. § 164.404(c)(2).
[23] Alabama, New Mexico, and South Dakota are the only states that have not yet adopted a data breach notification law.

the corresponding HIPAA requirement.[24] Although it is important to perform a comprehensive review of each state's breach notification requirements in order to determine how it will interact with HIPAA, a few common state law variations are worth mentioning:

Definition of "Personal Information": In many states, the scope of "personal information" is expanded to include electronic passwords, financial account information, license numbers, DNA profiles, and tax information.

Notice to Attorney General or State Agency: Most states require that notice also be given to the state attorney general's office or other state agency, such as the state police or consumer protection agency. This type of notification is often required only if the breach involves more than 500 individuals within the state.

Notification Within Specific Time Frames: A few state laws implement their own, more stringent, time requirement by which a covered entity must notify affected individuals. The most common variation is 45 days after discovery of the breach; however, the notification window can be as short as 30 days after discovery.

Private Cause of Action: Unlike HIPAA, a minority of states provide for a private cause of action for damages suffered as a result of a violation of the state's breach notification statute. These causes of action are often embedded within the state's deceptive trade practices statute and, in a few states, allow for treble damages to be awarded.

Consequences of Noncompliance

Failure to comply with the requirements of HIPAA can result in both criminal and civil penalties, as well as exclusion from federal programs, depending upon the nature and extent of the violation.[25]

Criminal Penalties

Any individual who (1) knowingly uses or causes to be used a unique health identifier, (2) obtains individually identifiable health information relating to an individual, or (3) discloses individually identifiable health information to another person may be subject to criminal sanctions.[26] Criminal penalties only apply when an individual acts knowingly, or purposefully.[27] The Department of Justice interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute the violation.[28] In other words, specific knowledge of an action being in violation of the HIPAA statute is not required for criminal liability to be imposed.[29]

In the case of any purposeful violation, a $50,000 fine may be imposed in addition to one year of imprisonment.[30] Individuals committing offenses under false pretenses may be subject to a

[24] 45 C.F.R. § 160.203.

[25] 42 U.S.C. § 1320d-5.

[26] 42 U.S.C. § 1320d-6(a).

[27] *Id*.

[28] United States Department of Justice, *Memorandum Opinion for the General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6* (June 1, 2005), http://www.justice.gov/sites/default/files/olc/opinions/attachments/2014/11/17/hipaa_final.htm.

[29] *Id*.

[30] 42 U.S.C. § 1320d-6(b)(1).

$100,000 fine and up to five years in prison.[31] Finally, if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the individual may be fined $250,000 and could face 10 years in prison.[32]

Civil Penalties

The American Recovery and Reinvestment Act of 2009 established a tiered civil penalty structure for HIPAA violations; however, the HHS secretary retains authority to modify the amount of the penalty based upon the nature and extent of the violation.[33] The secretary is prohibited from imposing civil penalties if the violation is corrected within 30 days of discovery, except in cases of willful neglect.[34]

Nature of HIPAA Violation	Minimum Penalty	Maximum Penalty
HIPAA violation where individual did not know (and would not have known through reasonable diligence) that he or she violated HIPAA	$100 per violation, subject to an annual maximum of $25,000 for repeat violations	$50,000 per violation, subject to an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, subject to an annual maximum of $100,000 for repeat violations	$50,000 per violation, subject to an annual maximum of $1.5 million
HIPAA violation due to willful neglect, but violation is corrected within the required time period	$10,000 per violation, subject to an annual maximum of $250,000 for repeat violations	$50,000 per violation, subject to an annual maximum of $1.5 million
HIPAA violation due to willful neglect and is not corrected	$50,000 per violation, subject to an annual maximum of $1.5 million	$50,000 per violation, subject to an annual maximum of $1.5 million

Although there is currently no private cause of action for individuals harmed by HIPAA violations, state attorneys general may bring civil actions and obtain damages on behalf of state residents.[35]

Exclusion

In extreme cases, the HHS secretary has the authority to exclude a provider from participation in any federal healthcare program for conduct relating to fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service.[36] While exclusion carries many consequences, the primary effect is

[31] 42 U.S.C. § 1320d-6(b)(2).
[32] 42 U.S.C. § 1320d-6(b)(3).
[33] *Id.*
[34] 42 U.S.C. § 1320d-5(b)(2)(A).
[35] 42 U.S.C. § 1320d-5(d)(1).
[36] Social Security Act, 42 U.S.C. § 1320a-7(b).

that the federal government will not provide payment for any items or services furnished, ordered, or prescribed by an excluded individual or entity.[37]

Obstruction of Justice

The failure to adequately investigate allegations of healthcare fraud can frequently lead to obstruction of justice charges. A criminal statute enacted as part of HIPAA provides that "[w]hoever willfully prevents, obstructs, misleads, delays or attempts to prevent, obstruct, mislead, or delay the communication of information or records relating to a violation of a federal health care offense to a criminal investigator" could be subject to civil penalties and/or up to five years in prison.[38]

Obstruction of justice charges are particularly concerning in the healthcare context because the underlying conduct that serves as the basis for the offense is often seemingly benign when compared with common forms of obstruction like jury tampering or destruction of evidence. For example, an innocent misstatement or an inadvertent failure to produce a responsive document in the course of an investigation may be construed as a willful obstruction. Additionally, given the complexity of many healthcare fraud schemes, obstruction of justice is often easier for the government to prove to a jury. It is, therefore, essential that healthcare providers put in place an effective internal investigation policy and process so that they are prepared to interact with government investigators in a manner that can only be construed as cooperative.[39]

Key Steps for Implementing an Effective Incident Response Plan

Once a breach has been detected, it is crucial that the covered entity immediately begin to execute its incident response plan. The first 24–72 hours after discovery are especially critical to the successful resolution of a data breach. In the event of a breach, healthcare providers should follow these key steps:

(1) Record key dates and times.

Record the date and time when the breach was discovered and confirmed, as well as the date and time when the incident response plan is initiated. This information should ultimately be compiled in an incident report.

(2) Assemble the incident response team and engage necessary external resources.

The incident response team is usually composed of both internal and external members, and should be formed in advance of any breach. Often the team is led by an internal or external legal department or a chief privacy officer, who is tasked with coordinating the response efforts among the various stakeholders.

It is essential for the covered entity to identify what breach response roles it will outsource based on the organization's available resources. Outside vendors can be hired to handle the legal, forensic, notification, public relations, and victim protection aspects of the breach response process. It is also important at this stage to establish a

[37] *See* U.S. Department of Health and Human Services, Office of Inspector General, Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs (May 8, 2013), http://oig.hhs.gov/exclusions/files/sab-05092013.pdf (additional consequences associated with exclusion).

[38] 18 U.S.C. § 1518.

[39] *See* 70 Fed. Reg. 4876 (2005) (OIG Supplemental Compliance Program Guidance for Hospitals).

communication protocol with the incident response team in case information about the breach is leaked prior to proper notification.

(3) Secure the premises and preserve evidence.

This step varies depending upon the nature and extent of the data breach. In general, it involves securing the premises where the breach occurred, taking inventory of missing items, reviewing surveillance data, and working with either law enforcement or private forensic experts to conduct the investigation. The incident response team should designate one member who is in charge of communicating directly with law enforcement personnel.

It is also important to disconnect any computers or electronic devices from the network in order to isolate the system from further harm, but refrain from turning them off to avoid the possibility that crucial evidence will be lost.

(4) Interview key custodians and identify compromised data.

After securing evidence, the incident response team should continue its investigation by interviewing key custodians of records to determine what data was compromised, how it was taken, by whom and to whom was the incident reported, and the potential risks associated with the exposure. Be sure to document all actions taken during the course of the investigation and pay particular attention to those aimed at determining the root cause of the breach. Regulators will always ask for evidence of action taken to determine the cause of the breach and to prevent further exposure.

(5) Conduct risk assessment.

After the necessary information has been gathered, it is imperative that the incident response team undertake an incident risk assessment using the four-factor analysis set forth in HIPAA's accompanying regulations. State law may require the consideration of additional factors in this analysis. Many third-party vendors offer services and tools to assist in this process. It is at this stage that a determination is made as to whether a breach triggers any of the federal or state notification requirements.

(6) Notify all necessary parties as soon as possible.

If the risk assessment determines that the breach is reportable, the covered entity should act swiftly to notify the necessary parties as required by both federal and state law. While federal and state notification deadlines can range from 30 to 60 days after discovery of a breach, a covered entity should not delay notification. The law requires that notification be given without unreasonable delay, and it is usually best practice to notify affected individuals as soon as possible. Since most organizations do not have the resources necessary to handle mass notifications, it is common for the covered entity to seek outside assistance by setting up a call center and customer relationship management system.

(7) Perform postbreach review and update incident response plan.

The sole advantage of experiencing a data breach is that it affords covered entities the opportunity to assess the effectiveness of their incident response plan and make any necessary revisions based on weaknesses that were highlighted during the previous

incident. Given the rapid pace at which the technology and legal landscape associated with the proper handling of data is changing, it is essential for healthcare providers to undertake a thorough and frequent review of their incident response plan.

Conclusion

Data breaches, particularly in the context of the provision of healthcare, can be frightening for both affected individuals and the entity tasked with securing the data. The healthcare sector is increasingly reliant on technology to store and transmit sensitive information. In addition, agencies tasked with ensuring compliance with federal and state privacy laws are stepping up their efforts. It is often only a matter of time before even the best healthcare providers are faced with the challenge of coordinating a proper response to a data breach.

It has never been more important for organizations involved in the provision of healthcare to ensure that they have an effective incident response plan in place in the event that a breach occurs. This plan should be carefully crafted after consideration of federal and state law, and should be regularly reviewed to ensure compliance with the current legal landscape. Once in place, a proper incident response plan can save a healthcare provider time, money, and, perhaps most importantly, its reputation.

Authors:

Mark A. Rush
mark.rush@klgates.com
+1. 412.355.8333

Patricia C. Shea
patricia.shea@klgates.com
+1. 717.231-5870

Eric M. Matava
eric.matava@klgates.com
+1. 412.355-7445