Bloomberg BNA

Tax Management
Compensation Planning Journal™

A Fresh Look at Privacy Rules in Light of Recent Cyberattacks in the Health Sector

By Sravya Boppana and Vivian Hunter Turner[1]

As the world becomes increasingly reliant on technology to store massive quantities of information and as access to this information becomes more global, cyberattacks have manifested themselves as a viable and menacing threat. Cyberattacks have impacted many industries including retail, entertainment, and health care, and they have been used to gather various kinds of information about not just the corporations, but also about the individuals that patronize or work for them. In this article, we focus on the increasing threat to the security of health information, legal requirements in place at the federal and state level to protect health information, and the consequences of a violation of these rules. We also provide a toolkit to help companies prevent and manage breaches that may compromise individuals' health information.

RECENT CYBERATTACKS

In the first three months of 2015, we have already seen two large-scale cyberattacks targeted at health insurance issuers that have compromised health-related information of approximately 90 million people in the United States. These attacks are on such a large scale and have such a broad impact that they dwarf prior reported breaches of health information.

Anthem

The first of these reports came in February, when health insurer Anthem announced that, through "a very sophisticated external cyberattack," hackers infiltrated a database containing records of approximately 80 million people.[2] Anthem reported that "tens of millions" of records may have been stolen, which if true, would make it the largest health care breach to have ever occurred.[3] Anthem further revealed that no diagnosis or treatment information was exposed; however, the hackers may have accessed individuals' names, dates of birth, member IDs, social security numbers, addresses, phone numbers, email addresses, and employment information.[4]

Premera

Following closely on the heels of Anthem's announcement, in March, Premera Blue Cross (Premera) announced that it, too, was the target of a sophisti-

[1] Sravya Boppana and Vivian Hunter Turner are attorneys at Groom Law Group, Chartered in Washington, D.C.

[2] Elizabeth Weise, *Millions of Anthem Customers Alerted to Hack*, USA Today (Feb. 5, 2015), http://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach/22917635/.

[3] *Id.*

[4] AnthemFacts.com, *Frequently Asked Questions*, https://www.anthemfacts.com/faq?utm_source=Anthem+February+Newsletter++Barbara&utm_campaign=Anthem+Newsletter+Barbara&utm_medium=email.

ISSN 0747-8607

cated cyberattack that may have affected 11 million people.[5] Premera reported that hackers may have gained access to personal information of its members, employees, and individuals with whom Premera does business.[6] Similar to the Anthem attack, Premera stated that compromised information may include individuals' names, dates of birth, member IDs, social security numbers, addresses, phone numbers, and email addresses.[7] In addition, the Premera attack may have resulted in compromised bank account information and claims information.[8]

Legal Consequences

While these two cases involved millions of individuals and received national media attention, even smaller disclosures or cyberattacks could trigger the myriad of laws that may require health plans or insurers to adopt safeguards or notify individuals or regulators of potential breaches. The privacy of health information is protected by a patchwork of different legal sources. At the federal level, the major applicable statute is the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'') and related regulations.[9] At the state level, constitutional principles, common law, and statutory requirements of several different states could apply to information breaches.

We go into more detail below on these various federal and state requirements.

HIPAA PRIVACY RULE

Until 1996, there was no comprehensive federal statute providing uniform rules regarding the privacy of health information. This changed with Congress's enactment of HIPAA, which, in part, aims to protect the security and ensure the confidentiality of health information. HIPAA generally requires that the Secretary of the Department of Health and Human Services issue standards regarding the privacy, security, and electronic exchange of health information.[10]

In accordance with this requirement, in 2000, the Department of Health and Human Services (HHS) published the Privacy Rule.[11] In 2009, HHS further expanded protections and liability under HIPAA through the Health Information Technology for Economic and Clinical Health Act (HITECH Act),[12] which was issued as a part of the American Recovery and Reinvestment Act.

The Privacy Rule provides rights to individuals and imposes obligations on certain entities that may hold individually identifiable health information. The Privacy Rule specifies the entities to which its protections apply, the types of information that are accorded protection, the limited instances in which disclosure is permitted or required, and what happens in the event that the Privacy Rule is breached.

Entities Subject to HIPAA

Not all entities that may hold individual health information are subject to the requirements of HIPAA. In fact, HIPAA only applies to three types of entities: 1) health plans; 2) certain health care providers; and 3) health care clearinghouses.[13] These entities are known as ''covered entities.''[14]

Health Plans. Health plans are generally subject to the Privacy Rule with very limited exceptions. Under HIPAA, individual and group plans — whether fully insured or self-funded — are covered entities if they provide a health benefit (such as health, dental, vision, prescription drug, EAP or health FSA benefit).[15]

Only a limited number of plans expressly fall outside this general rule:

- benefits that fall under the ''first'' category of HIPAA ''excepted benefits'' under PHSA 2791(c)(1) — workers' compensation, automobile, property and casualty insurance, disability, and on-site medical clinics;[16]
- plans with less than 50 participants that are administered solely by the sponsoring employer;
- government-funded programs with a principal purpose other than providing for, or paying the cost of, health care; and
- government-funded programs with a principal activity to directly provide health care or make

---

[5] PremeraUpdate.com, *Premera Has Been the Target of a Sophisticated Cyberattack*, http://www.premeraupdate.com/.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Note that when we refer to ''HIPAA'' in this article and the entities subject to HIPAA, we are referring only to the HIPAA Privacy & Security Rules, unless stated otherwise. There are separate regulations that apply to other requirements under HIPAA, such as rules related to portability, Affordable Care Act protections, and nondiscrimination and wellness.

[10] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, §264(c)(1).

[11] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. Parts 160 & 164).

[12] Pub. L. No. 111-5, Div. A, §13405.

[13] 45 C.F.R. §160.102(a).

[14] 45 C.F.R. §160.103.

[15] *Id.*

[16] 42 U.S.C. 300gg-91(c)(1). Note that other HIPAA-excepted benefits are subject to the HIPAA Privacy Rules, including employee assistance programs, dental and vision plans, long-term care plans, disease-only policies, fixed indemnity plans, and supplemental benefits.

ISSN 0747-8607

grants to fund the direct provision of health care.[17]

It is important to note that for group health plans, the distinction between the health plan and the employer is crucial. Under HIPAA, the health plan is a separate legal entity from the employer. While the health plan is subject to the requirements of HIPAA, the employer, in its capacity as the employer or plan sponsor, generally is not. The definition of ''protected health information'' under HIPAA excludes health information held by the employer in its employer capacity. Thus, to the extent that an employer holds health information, such as sick leave or performance reports, in its capacity as an employer, and where it does not obtain this information from the health plan, such information would not be subject to HIPAA's privacy requirements. However, where the employer is acting on behalf of the health plan or has obtained the information from the health plan, HIPAA would continue to apply.

Health Care Providers. Health care providers are also bound by HIPAA's requirements to the extent that they electronically transmit or use a third party to electronically transmit health information with respect to claims, benefit eligibility inquiries, referral authorizations, and other transactions that HHS has stated are standard transactions.[18] Such health care providers are subject to HIPAA regardless of their size, and whether they are institutional (e.g., hospitals) or non-institutional (e.g., physicians).[19]

Health Care Clearinghouses. Finally, health care clearinghouses, which are entities that process nonstandard information from another entity into standard data elements or vice versa, are subject to HIPAA.[20] Health care clearinghouses include billing systems or community health management systems.

The covered entities described above must comply with HIPAA's requirements to ensure that health information remains secure and, if health information is breached, follow certain breach protocols set forth under HIPAA.

Information Protected by HIPAA

HIPAA's Privacy Rule protects ''protected health information,'' which is health information that is: (1) created or received by a covered entity or employer and relates to the physical or mental health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual; and (2) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[21] The Privacy Rule protects health information to the extent that it is individually identifiable or to which there is a reasonable basis to believe that the information can be used to identify the individual.[22] If health information is de-identified completely, meaning it has been stripped of all of the identifiers listed in the Privacy Rule, or a person with appropriate knowledge has certified that the information cannot be used to identify an individual who is a subject of the information, then such information may be outside the scope of HIPAA.[23]

Clearly, protected health information includes claims information, diagnostic information, treatment information, and payment history. However, based on reports and statements made by the HHS Office of Civil Rights (OCR), it seems that the protections of HIPAA may apply to a broader set of information. In its Annual Report to Congress, OCR reported that some of the small breach reports received by the HHS related to the mailing of member ID cards to the wrong individuals.[24] Consistent with this position, in relation to a breach in which a pharmacy employee placed a customer's insurance card in another customer's prescription bag, ''OCR clarified that an individual's health insurance card meets the statutory definition of protected health information and, as such, needs to be safeguarded.''[25]

The OCR's broad interpretation of ''protected health information'' could have significant implications. In some of the recent attacks, only member ID numbers may have been compromised. It appears that HHS may consider even this information to be protected health information subject to HIPAA's breach rules.

---

[17] 45 C.F.R. §160.103.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *See* 45 C.F.R. §160.103.

[23] 45 C.F.R. §164.502(d)(2), §164.514(a), §264.514(b). *See* HHS, Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability (HIPAA) Privacy Rule (Nov. 26, 2012), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html.

[24] HHS Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf.

[25] HHS, Enforcement Activities & Results, Case Examples & Resolution Agreements, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html.

ISSN 0747-8607

The Privacy Rule's Protections

As discussed above, the Privacy Rule operates by providing rights to individuals and imposing requirements on covered entities.[26]

Individual Rights. HIPAA provides individuals with certain rights: (1) the right to a covered entity's notice of privacy practices; (2) the right to access protected health information; (3) the right to amend protected health information; (4) the right to restrict protected health information; (5) the right to request confidential communications; and (6) the right to an accounting of certain disclosures of protected health information made by a covered entity.

Right to a Covered Entity's Notice of Privacy Practices. Under HIPAA, an individual has a right to notice of the uses and disclosures of protected health information that may be made by a covered entity.[27] In addition, individuals have the right to be notified of their rights and the covered entity's legal duties with respect to their protected health information.[28] Generally, if a group health plan is self-funded, then the plan itself must provide such notice to the individual, and if a group health plan is insured, then the health insurance issuer must provide the notice.[29] The notice must be provided upon enrollment or when a covered entity makes any material changes to its privacy practices. A notification of the availability of the full notice must be provided every three years. Many plans provide this notice as part of their annual enrollment materials or annual summary plan description, but the notice itself may not be accompanied by an authorization form.[30] In addition to distribution of the notice, if a health plan maintains a website regarding benefits, the notice must be posted to the website.[31]

Right to Access Protected Health Information. HIPAA provides individuals the right to inspect and obtain copies of their protected health information that is maintained in a ''designated record set,'' which is a group of records maintained by or for a covered entity that includes medical records, billing records, enrollment information, payment information, or claims information, and is used in whole or part to make decisions about individuals.[32] Individuals can request their records in hard copy or electronic form. Covered entities generally have 30 days to act on the request by providing a copy of the record or providing a written denial of the request.

Right to Amend Protected Health Information. Individuals have a right to request an amendment to their protected health information. A covered entity may deny the request if certain conditions are met, such as if the covered entity disagrees with the amendment or did not originate the information.[33] Further, covered entities have discretion to require that requests be made in writing and include a reason for the requested amendment.[34] A covered entity generally must respond to the individual's request within 60 days.[35]

Right to Restrict Protected Health Information. HIPAA provides that a covered entity must permit individuals to request the covered entity to restrict uses and disclosures of their protected health information.[36] However, a covered entity is not required to actually agree to the restriction unless the disclosure is to carry out payment or health operations and is not otherwise required by law, and the protected health information pertains solely to an item or service for which the covered entity has been paid in full by the individual or by a person other than the health plan on behalf of the individual.[37] For example, if an individual has paid out of pocket in full for a certain service, he or she may request that the covered entity not disclose information about that service, even for treatment, payment, or health care operations purposes.

Right to Request Confidential Communications. In addition, an individual can request that the covered entity send communications to an alternative confidential address.[38] The covered entity is required to comply if the individual states that he or she would be in danger from the prior means of communications (for example, in a domestic violence situation, a spouse may request that claims reports be sent to an alternative address).[39]

Right to an Accounting of Disclosures of Protected Health Information. Finally, HIPAA provides individuals the right to receive an accounting of disclosures of their protected health information made by a covered entity, with certain limited exceptions, in the six years prior to the date of the request.[40] The accounting must be in writing, include disclosures to or by the covered entity's business associates, and state

---

[26] This article provides an overview of the primary requirements of the HIPAA privacy and security rules. More detail can be found in the regulations themselves at 45 C.F.R. Parts 160–164.

[27] 45 C.F.R. §164.520(a)(1).

[28] *Id.*

[29] 45 C.F.R. §164.520(a)(2).

[30] 45 C.F.R. §164.508(b)(3).

[31] 45 C.F.R. §164.520(c)(3).

[32] *See* 45 C.F.R. §164.524. *See also* 45 C.F.R. §164.501.

[33] 45 C.F.R. §164.526(a).

[34] 45 C.F.R. §164.526(b).

[35] *Id.*

[36] 45 C.F.R. §164.522(a)(1).

[37] 45 C.F.R. §164.522(a)(1)(ii), §164.522(a)(1)(vi).

[38] 45 C.F.R. §164.522(b)(1)(i).

[39] 45 C.F.R. §164.522(b)(1)(ii).

[40] 45 C.F.R. §164.528(a).

ISSN 0747-8607

the date of the disclosure, the name of the person who received the protected health information, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure.[41] Notably, the accounting does not have to include disclosures for routine treatment, payment, or health care operations purposes or disclosures pursuant to an individual's authorization.[42]

Requirements Imposed on Covered Entities. In addition to ensuring that they do not restrict individuals' rights under HIPAA, covered entities are also subject to independent obligation under HIPAA.

Use and Disclosure Rules. Generally, HIPAA requires that a covered entity obtain the individual's written authorization to use or disclose protected health information, except where the disclosure is for the purpose of treatment, payment, or health care operations of the covered entity.[43] These are defined terms under the Privacy Rule. For example, a health plan may disclose protected health information without authorization to determine eligibility, administer claims, or conduct underwriting.

Even for these routine treatment, payment, and health care operations purposes, a covered entity generally must make reasonable efforts to use or disclose only the minimum amount of protected health information that is necessary for the purpose.[44]

The Privacy Rule requires disclosure upon an individual's request pursuant to his or her rights to access protected health information and to an accounting of disclosures of protected health information (as described above).[45] In addition, the Privacy Rule permits use and disclosure of protected health information without an authorization for certain exceptions, such as where required by law, subject to judicial process, or for a public interest, such as to respond to an audit inquiry or to report abuse.

For other uses and disclosures, a covered entity generally must obtain the individual's authorization.[46] The authorization must be in writing and contain specific language regarding the information to be used or disclosed, the entity disclosing or receiving the information, when the authorization expires, and the individual's right to revoke the authorization.[47]

Business Associates. As discussed above, the requirements of HIPAA apply to covered entities. However, in reality, access to health information does not always end with the covered entity. For example, health plans often contract with other entities, such as third-party administrators, who process claims and make available networks of providers (TPAs), as well as law firms, consultants, and actuarial firms, to assist with business functions. Depending on the nature of services they provide, these third parties may have access to health information that is protected under HIPAA.

Under HIPAA, a business associate is an entity that performs functions on behalf of or services for a covered entity that may involve the use or disclosure of protected health information.[48] Business associates can be entities that assist with claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management or repricing, or that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a covered entity.[49]

HIPAA requires covered entities to enter into ''business associate agreements'' with these business associate service providers that may have access to protected health information.[50] Business associate agreements generally provide that the business associate will comply with the requirements of HIPAA and require the business associate to impose the same compliance obligations on any sub-contractor that the business associate may engage that also will access the covered entity's protected health information.

Documentation and Procedures. HIPAA requires that covered entities document a number of items related to compliance under the rules, including formal policies and procedures, authorization requests, and a record of any potential breaches. Specifically, for group health plans, HIPAA requires that, if the plan will disclose protected health information to the plan sponsor, the plan document be amended to, among other things, allow the disclosure and require that the plan sponsor also certify that it will safeguard the information.[51]

Further, under HIPAA, covered entities must also implement policies and procedures regarding protected health information that are reasonably designed to ensure compliance with HIPAA's requirements.[52] Whether a policy is ''reasonably designed'' depends on a number of factors, including the size and type of activities that the covered entity will undertake with respect to protected health information.

---

[41] 45 C.F.R. §164.528(b).
[42] 45 C.F.R. §164.528(a).
[43] 45 C.F.R. §164.508(a)(2).
[44] *See generally* 45 C.F.R. §164.502(b), §164.514(d).
[45] 45 C.F.R. §164.502(a)(2).
[46] 45 C.F.R. §164.508(a)(1).
[47] 45 C.F.R. §164.508(c).
[48] 45 C.F.R. §160.103.
[49] *Id.*
[50] *Id.*
[51] 45 C.F.R. §164.504(f)(2).
[52] 45 C.F.R. §164.530(i)(1).

ISSN 0747-8607

Appointment of Privacy Official and Training of Workforce. Finally, HIPAA requires that covered entities designate a privacy official to be responsible for the development and implementation of the policies and procedures related to HIPAA's requirements.[53] In addition, a covered entity must designate a contact person or department that is responsible for receiving HIPAA-related complaints and who can provide further information about HIPAA-related matters.[54]

The covered entity also must determine which employees are part of its ''workforce'' that may access protected health information. The covered entity must train all members of its workforce on its policies and procedures regarding protected health information.[55] This applies to current members of the workforce as well as individuals who may be hired in the future.

Consequences of Breach of Privacy Rule. If a covered entity experiences a disclosure of protected health information that is not permitted or required by HIPAA, either on its own or by a business associate, the covered entity must determine whether the disclosure rises to the level of a ''breach'' under the rules, triggering certain notice requirements.

A breach is ''reportable breach'' under HIPAA if there is an acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA's Privacy and Security Rules that has ''compromised'' the security or privacy of such protected health information.[56] If a breach meets these requirements, a covered entity must report the breach to the individuals affected (as well as HHS and the media, if applicable) *unless* the covered entity can demonstrate that there is a low probability that protected health information has been compromised.[57] HIPAA requires that the determination of a reportable breach include consideration of:

> The nature and extent of protected health information involved;
>
> The unauthorized person who used the protected health information or to whom the disclosure was made;
>
> Whether protected health information was actually acquired or viewed; and
>
> The extent to which risk has been mitigated.[58]

A covered entity must document its findings in a risk assessment, even if it determines that a reportable breach has not occurred.[59] If there is a reportable breach, then a covered entity must:

> Notify the individuals whose protected health information is at issue no later than 60 days after discovery of the breach.[60] If the breach is on the part of the business associate, the business associate has 60 days to notify the covered entity, who then has 60 days to notify the affected individuals;[61]
>
> Immediately notify HHS if the breach involves 500 or more people. The preamble to the Privacy Rule indicates that this notice must be provided within 60 days. If the breach involves less than 500 people, the covered entity must record the incident on its breach log and file the log with HHS annually by March 1st;[62] and
>
> Immediately notify the media (within 60 days) if the breach involves more than 500 residents in a state.[63]

In addition to ensuring compliance with the breach notification rules, a covered entity also should maintain a written copy of the risk analysis as well as retain any documents related to the breach for a period of six years.

Though HIPAA places the responsibility following a breach upon covered entities, there is nothing in HIPAA precluding covered entities from delegating applicable reporting obligations to their business associates. Indeed, through business associate agreements, covered entities and business associates frequently address which party is responsible for costs of reporting, notification, and/or providing any additional protections.

HIPAA SECURITY RULE

Congress included provisions in HIPAA addressing the need for the security of any health information pertaining to an individual that is electronically maintained or transmitted. HIPAA added Title XI to the Social Security Act, which outlines standards for covered entities that transmit any health information in electronic form in connection with a HIPAA standard transaction — such as an eligibility file or an enroll-

[53] 45 C.F.R. §164.530(a)(1)(i).
[54] 45 C.F.R. §164.530(a)(1)(ii).
[55] 45 C.F.R. §164.530(b)(1)–§164.530(b)(2).
[56] *See* 45 C.F.R. §164.402.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] 45 C.F.R. §164.404(b).
[61] 45 C.F.R. §164.404(b), §164.410(b).
[62] 45 C.F.R. §164.408.
[63] 45 C.F.R. §164.406.

ISSN 0747-8607

ment file.[64] These rules have been codified at subpart C of Part 164 of the Code of Federal Regulations and are commonly referred to as the Security Rule.[65]

The HIPAA Security Rule and the Privacy Rule are inextricably linked. The protections of the privacy of information depend in large part on the existence of security measures to protect that information in electronic form. However, there are important distinctions between the Privacy Rule and the Security Rule.

The Security Rule requires administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The standards require covered entities to implement basic safeguards to protect electronic protected health information from unauthorized access, alteration, deletion, and transmission. The Privacy Rule, by contrast, sets standards for how protected health information should be controlled by setting forth what uses and disclosures are authorized or required and what rights individuals have with respect to their health information.

The scope of the Security Rule is more limited than that of the Privacy Rule. The Privacy Rule applies to protected health information in any form, where the Security Rule applies only to protected health information in electronic form.[66]

The HIPAA Security Rule requires that covered entities have certain security standards in place to comply with the statutory requirement that electronic protected health information is protected to ensure its privacy and confidentiality when it is electronically stored, maintained, or transmitted.[67]

Who Is Required to Comply?

The Security Rule applies to a covered entity that electronically maintains or transmits any health information relating to an individual.[68] Before the HITECH Act, the HIPAA Security Rule directly applied only to health covered entities and did not apply to business associates of covered entities. However, section 13401 of the HITECH Act 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. This means that business associates may be civilly and criminally liable for violations of these Security Rule provisions.[69]

While business associates had not been directly liable before the HITECH Act, they did have to comply with the Security Rule provisions through their business associate agreements with covered entities. These agreements required business associates to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that they create, receive, maintain or transmit on behalf of the covered entity and to ensure that any agent, including a subcontractor, to whom they provide such information agreed to the same safeguards.

Overview: What Is the Security Rule?

The HIPAA Security Rule is essentially a set of requirements that business associates and covered entities must include in their operations to assure that electronic protected health information pertaining to an individual remains secure. While the standards address specific aspects of the requirements, they generally do not reference or advocate specific technology. This allows the security standard to be ''flexible enough to take advantage of state-of-the-art technology.''[70]

In addition, as described more below, the standards are either ''required,'' in which case they are mandated, or ''addressable,'' in which case the covered entity will have to determine, based on its own circumstances, whether the standard is relevant. The standards do not address the extent to which a particular entity should implement the specific features. Instead, they require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.[71]

The Preamble to the Proposed Rule published in 1998 provides that ''[i]nherent in this approach is a balance between the need to secure health data against

---

[64] Section 1173(a) of Social Security Act, 42 U.S.C. 1320d-2. Title XI of the Social Security Act is administered by the Department of Health and Human Services and by the Department of Labor.

[65] 45 C.F.R. §164.302 *et seq.*

[66] *See* 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003) (preamble to final rules).

[67] *See* 68 Fed. Reg. 8334 (Feb. 20, 2003).

[68] *See* 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).

[69] *See* 45 C.F.R. §164.302 (''[a] covered entity or *business associate* must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity'' (emphasis added)).

[70] 63 Fed. Reg. 43,242, 43,249 (Aug. 12, 1998) (preamble to proposed rules that were subsequently finalized by 68 Fed. Reg. 8334 (Feb. 20, 2003)).

[71] 63 Fed. Reg. 43,242, 43,250 (Aug. 12, 1998).

ISSN 0747-8607

risk and the economic cost of doing so.''[72] The HITECH Act final regulations further provide that ''[c]overed entities and business associates have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any Security Rule standard.''[73]

The HIPAA Security Rule outlines a set of security standards that consist of requirements that a business associate or covered entity must address in order to safeguard the integrity, confidentiality, and availability of its electronic data. It also describes the implementation features that must be present in order to satisfy each requirement. The HIPAA Security Rule is divided into three broad categories: (1) administrative procedures; (2) physical safeguards, and (3) technical security services and mechanisms to prevent unauthorized access to data that is transmitted over a communications network.

Adopting Standards

The Security Rule outlines a set of standards that a health plan must follow. The rule adopts implementation specifications that provide instructions for implementing those standards. In some cases, the standard itself includes all the necessary instructions for implementation. In these instances, there may be no corresponding implementation specification for the standard specifically set forth in the regulation text, so the standards themselves also serve as the implementation specification. In other words, in those instances, the regulators adopted one set of instructions as both the standard and the implementation specification.[74]

Addressable Versus Required Standards

The Security Rule provides two types of implementation specifications, required and addressable. It provides that ''required'' implementation specifications must be met. However, with respect to implementation standards that are ''addressable,'' the Security Rule specifies that covered entities and business associates must assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, which may include consideration of factors such as: (1) the size and capability of the organization; (2) the entity's risk analysis; (3) risk mitigation strategy; (4) what security measures are already in place; and (5) the cost of implementation.

Essentially, the HIPAA Security Rule requires covered entities and business associates to evaluate an addressable standard and make one of three conclusions:

> If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity or business associate must implement it.
>
> If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the covered entity or business associate, but the standard cannot be met without implementation of an additional security safeguard, the covered entity or business associate may do one of two things:
>
> > Implement an alternate measure that accomplishes the same end as the addressable implementation specification; or
> >
> > If the standard can otherwise be met, the covered entity or business associate may choose not to implement the implementation specification or any equivalent alternative measure at all. The entity must document the rationale behind not implementing the implementation specification.[75]
> >
> > For example, encryption is an ''addressable'' standard. A covered entity may review the types of information it retains or transmits, along with its existing privacy protections, and determine that, in some cases, encryption is not necessary because the type of protected health information involved may not be as sensitive and the existing protections are sufficient to protect the information. As noted above, the covered entity would need to document this determination in its risk assessment.
>
> A covered entity or business associate may also decide that a given implementation specification is not applicable to its situation and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity or business associate must document the decision not to implement the addressable specification, the rationale behind its

[72] *Id.*

[73] 78 Fed. Reg. 5566, 5589 (Jan. 25, 2013) (preamble).

[74] 68 Fed. Reg. 8334, 8336 (Feb. 20, 2003).

[75] 68 Fed. Reg. 8334, 8341 (Feb. 20, 2003).

ISSN 0747-8607

decision, and how the standard is being met.[76]

Business Associate Agreement & Group Health Plan Amendment

The business associate agreement, required under the Privacy Rule, also must address the Security Standards. Similar to the Privacy Rule, the Security Rule outlines provisions that are required in a business associate agreement and generally requires that the business associate comply with the applicable provisions of the Security Rule, ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of the Security Rule and report to the covered entity any security incident of which it becomes aware.[77]

As under the Privacy Rule, business associates must agree that they will require their subcontractors also to agree to these restrictions. This means that business associates essentially must have a business associate agreement with their subcontractors with the same general provisions as the business associate agreement.

Similarly, the Security Rule requires that the plan amendment required under the Privacy Rule, which allows the health plan to disclose protected health information to the plan sponsor, be updated to reflect the Security Rule as well.

Security Standards

The Implementation Specifications under the Security Rule generally fall under three main areas: Administrative Safeguards, Physical Safeguards, and Technical Safeguards.

Administrative Safeguards. The Security Rule requires the adoption of administrative procedures to guard the integrity, confidentiality and availability of protected health information. These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.

The rule has four required elements: (1) completion of a written assessment of potential risks and vulnerabilities to electronic protected health information, commonly referred to as a ''security risk assessment''; (2) implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; (3) application of appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate; and (4) implementation of policies and procedures to regularly review records of information system activity, such as audit logs and access reports.[78]

As a practical matter, covered entities and business associates should have written documentation of compliance with the elements outlined above. In many cases, an entity's information technology systems may comply with the requirements outlined in the Security Rule due to existing corporate information technology practices. However, the Security Rule requires that covered entities and business associates have a written security risk analysis. The covered entity or business associate should review the required and addressable standards and, for each one, indicate either what current procedures they have that comply or why compliance is not necessary. For addressable standards, this would be where the covered entity or business associate notes alternative measures to comply. Where the covered entity or business associate finds ''gaps'' in procedures, they may need to implement a new safeguard in order to comply with the requirements.

Physical Safeguards. Second, the Security Rule requires covered entities and business associates to adopt physical safeguards to protect electronic health information. Physical safeguards relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.[79]

There are three main components to the Security Rule's physical safeguard requirement:

> Facility access control addresses procedures to limit physical access to the information system and the facility in which it is housed and that access to the facility is controlled and validated based on an individual's role or function;
>
> Workstation use and security addresses procedures to specify physical attributes and safeguards of a workstation that can access electronic protected health information and implements physical safeguards for workstations that access electronic protected health information; and
>
> Device and media controls address procedures to govern receipt and removal of hard-

[76] *Id.*; 63 Fed Reg. 43,242, 43,250 (Aug. 12, 1998).
[77] 45 C.F.R. §164.314.
[78] 45 C.F.R. §164.308.
[79] 63 Fed. Reg. 43,242, 43,250 (Aug. 12, 1998).

ISSN 0747-8607

ware and electronic media that contain electronic protected health information within the facility and outside the facility.[80]

Technical Safeguards. Third, the Security Rule requires covered entities and business associates to adopt technical safeguards to protect electronic protected health information. Technical safeguards are the technology and policy and procedures for the use of electronic protected health information that protect electronic protected health information and control access to it. As noted above, the Security Rule does not identify specific requirements for the types of technology to implement. Rather, the Security Rule allows a covered entity to use any security measure that allows it to reasonably and appropriately implement the standards and implementation specifications.

The Security Rule outlines five technical security service requirements with supporting implementation features: (1) access control; (2) audit control; (3) integrity; (4) person or entity authentication; and (5) transmission security.[81]

Policies and Procedures

In addition to documenting the security risk assessment of the covered entity's compliance with the implementation specification, the covered entity or business associate must establish policies and procedures implementing the Security Rule's requirements.[82] The policies and procedures should ''reflect the mission and culture of the organization. . .[and] may be modified as necessary to meet the changing needs of an organization, as long as the changes are documented and implemented in accordance with the Security Rule.''[83] For most covered entities and business associates, the Security Procedures will overlap with the Privacy Procedures (and may be the same document). In some cases, a company already may have corporate security procedures that also can serve as the HIPAA Security Procedures.

The Security Rule requires covered entities to: (1) maintain the policies and procedures for six years; (2) train their workforces on the procedures and make the procedures available; and (3) update as needed in response to environmental or operational changes affecting the security of the electronic protected health information.

STATE PRIVACY PROTECTIONS

While HIPAA is a uniform federal law, it does not automatically preempt state laws pertaining to privacy or security of health information. In fact, HIPAA only preempts state laws that are ''contrary to'' HIPAA, meaning state laws where it would be impossible to comply with both HIPAA and the state law or the state law would be an obstacle to the accomplishment of HIPAA.[84] Generally, state privacy or security laws that are more stringent than HIPAA are not preempted.[85] For example, if HIPAA requires a breach notice to be provided within 60 days, and state law requires a breach notice to be provided within 30 days, it would be possible to comply with both, so the two laws would not be ''contrary.'' The state law would not be preempted.

As such, in addition to complying with HIPAA's requirements, covered entities must ensure that they are compliant with applicable state laws. State laws can exist as common law principles developed through case law over time or as statutory requirements. Common law principles that are often cited in cases relating to privacy of information include breach of contract, breach of fiduciary duties, and invasion of privacy. Case law can be very well-developed; however, because it is shaped by individual cases, the rules under state common law can vary drastically from state to state. State statutory requirements protecting privacy of information also can be very different in each state.

Several states have specific laws addressing personal financial information. These laws could apply to covered entities or more broadly, such as to employers or anyone doing business in the state. If these state laws are not contrary to HIPAA, then both sets of laws could apply. For example, California has laws that address health information, such as an individual's medical history, condition, or treatment.[86] However, California also has laws protecting social security numbers, driver's license numbers, bank information, and health insurance policy numbers or identification numbers as protected ''personal information'' in combination with an individual's first name or initial and last name.[87] This law would apply not only to HIPAA-covered entities, but to businesses generally.[88] Similarly, in Washington, social security numbers, driver's license numbers and bank information are

[80] 45 C.F.R. §164.310.

[81] 45 C.F.R. §164.312.

[82] 45 C.F.R. §164.316.

[83] Summary of the HIPAA Security Rule, Organizational Requirements, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

[84] 45 C.F.R. §160.203.

[85] 45 C.F.R. §160.203(b).

[86] Cal. Civil Code §1798.80–§1798.84.

[87] *Id.* §1798.80(e).

[88] Cal. Civil Code §1798.80(a).

ISSN 0747-8607

considered personal information in combination with an individual's first name or initial and last name.[89]

ENFORCEMENT: DEPARTMENT OF HEALTH AND HUMAN SERVICES

Corrective Action Plans and Fines and Penalties

There are two essential enforcement schemes under HIPAA: (1) sanctions that the group health plan may impose; and (2) criminal and civil penalties that the Department of Justice and HHS, respectively, may impose.

[89] Wash. Rev. Code §19.255.010(5). This type of information also could be considered protected health information under HIPAA if held by a covered entity.

Sanctions. HIPAA requires covered entities to apply appropriate sanctions against ''workforce'' members who violate the plan's privacy procedures.[90] HIPAA does not specify what sanctions the plan must impose, so the plan is able to determine what sanctions are appropriate. Appropriate sanctions may be determined at the time of the violation, allowing the plan to take into account the circumstances of the violation and the best way to improve compliance.[91] HIPAA requires that the group health plan document any sanctions that are applied.[92]

Civil Monetary Penalties. Separate from the covered entity's internal sanctions, HHS may impose civil monetary penalties for violations of HIPAA. The HHS prepared the table below to highlight the penalty amounts.

[90] 45 C.F.R. §164.530(e).

[91] 65 Fed. Reg. 82,462, 82,747 (Dec. 28, 2000).

[92] 45 C.F.R. §164.530(e).

Categories of Violations and Respective Penalty Amounts Available		
Violations Category	**Each Violation**	**All such violations of an identical provision in a calendar year**
Did Not Know	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect	$10,000 – $50,000	$1,500,000
Willful Neglect — Not Corrected	$50,000	$1,500,000

In assessing the amount of civil monetary penalties, HHS is required to base such determination on the nature and extent of the violation and the nature and extent of the harm resulting from such violation. As noted in the first column, the amount of civil monetary penalties is based on the culpability of the violator. The lowest tier, in which the penalty ranges from $100 to $50,000 for each violation, is for violations in which a group health plan ''did not know'' and by exercising due diligence would not have known that they violated HIPAA. In contrast, the highest tier is reserved for violations due to ''willful neglect'' that were not corrected. The highest penalty in this tier is $50,000 per violation, and the total penalty is capped at $1.5 million for violations of an identical requirement.[93]

HIPAA provides three exceptions to the imposition of civil penalties: (1) violations that are punishable as criminal offenses under HIPAA; (2) violations that occurred despite the exercise of ordinary business care and prudence to comply with HIPAA that was not due to willful neglect; and (3) violations that occurred that were not due to willful neglect and were corrected either during the 30-day period beginning on the first date the group health plan knew of the violation (or would have known by exercising reasonable diligence) or an additional reasonable period determined by HHS.[94]

Criminal Penalties. The United States Department of Justice has the authority to enforce HIPAA's criminal penalties.[95] The criminal penalties apply, in relevant part, to health plans and — depending on the facts of a given case — certain directors, officers, and employees of these entities in accordance with general principals of corporate criminal liability.[96] HIPAA prescribes criminal sanctions only for those violations

[93] 45 C.F.R. §160.404(b).

[94] 45 C.F.R. §160.410.

[95] 68 Fed. Reg. 18,895, 18,896 (Apr. 17, 2003).

[96] Memorandum Opinion for the General Counsel Department of Health and Human Services and Senior Counsel to the Deputy

ISSN 0747-8607

of the standards that involve the disclosure of protected health information.[97]

HIPAA also prescribes a tiered scheme for criminal penalties. A violation is punishable generally as a misdemeanor by a fine of not more than $50,000 and/or imprisonment for not more than one year.[98] Certain aggravating circumstances may make the offense a felony. The statute's highest penalties — a fine of not more than $250,000 and/or imprisonment of not more than 10 years — are reserved for offenses committed ''with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm.''[99]

TOOLKIT

HIPAA outlines a complex maze for covered entities to navigate. The list below provides a high-level overview of action steps a covered entity can take to comply with the HIPAA Privacy & Security Rule. These steps can be useful in helping employers to prevent, or perhaps mitigate the damage from, the cyberattacks outlined at the beginning of this article.

Document HIPAA Training and Update It to Reflect the HITECH Act

While HIPAA requires that a covered entity train its workforce, it does not prescribe a timeline to update its training. As discussed above, the HITECH Act strengthened many of the protections that existed when HIPAA was first promulgated. In light of the HITECH Act's sweeping changes, covered entities should update their HIPAA training materials and provide refresher training for their workforce. In addition, covered entities should review which individuals within their workforce may have access to protected health information and may need training. For example, along with the benefits group, the IT department may occasionally access protected health information. Employees also may transfer to other departments. Covered entities may want to ''cast a wide net'' when determining which individuals should be trained.

Adopt a Set of HIPAA Policies and Procedures Addressing Both the Security Rule and the Privacy Rule and Update Them for Changes to Reflect the HITECH Act

When regulations for HIPAA were first promulgated, many covered entities created or purchased a template set of policies and procedures that may not have been tailored to fit their organization's needs — or may not have been updated as their needs evolved. Covered entities should update their HIPAA policy and procedure for new requirements, such as the security breach rule, and to reflect the plan's actual procedures and particular issues. In addition, covered entities should make sure that these procedures are followed. For example, if the procedures require that filing cabinets that store protected health information are locked at night, the covered entity can make sure that this safeguard actually is being used. Covered entities also should make sure that their procedures include security of electronic protected health information, as well as privacy protections. Many covered entities adopted privacy procedures, but failed to update their procedures when the Security Rule was issued.

Appoint a HIPAA Privacy Officer and HIPAA Security Officer

Covered entities should make sure that a HIPAA Privacy Officer and a HIPAA Security Officer have been formally appointed. HIPAA allows the Privacy and Security Officer to be the same individual, different individuals, or even a team of individuals. As a practical matter, HIPAA does not prescribe how the Privacy and Security Officer should be appointed. Many covered entities designate the Privacy and Security Officer in their HIPAA Policies and Procedures and update the designation as the individual(s) in this role change over time. The covered entity's privacy and security training should include the names of the Privacy and Security Officers in case workforce members have additional questions.

Identify Business Associates and Enter into Business Associate Agreements

Covered entities should review vendors that have executed business associate agreements and confirm whether new vendors should be added to the list (for business associates, this may mean new business associate agreements with subcontractors). Covered entities should make sure that business associate agreements reflect revisions that were required by the HITECH Act.

Conduct a HIPAA Security Risk Assessment

Covered entities should review and update the HIPAA security assessment related to electronic protected health information (note that this requirement would apply to business associates as well, because

---

Attorney General (June 1, 2005), http://www.justice.gov/olc/opinion/scope-criminal-enforcement-under-42-usc-1320d-6.

[97] 42 U.S.C. §1320d-6(a).

[98] 42 U.S.C. §1320d-6(b)(1).

[99] 42 U.S.C. §1320d-6(b)(3).

ISSN 0747-8607

the HITECH Act made them directly liable under the HIPAA security standards). The risk assessment should be maintained in writing for six years. HHS has materials available on its website that provide information on the HIPAA Security Rule and answer many commonly asked questions.

CONCLUSION

As President Obama recently said, ''. . . it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm.''[100] The recent attacks have heightened the awareness of the need to adequately protect electronic health information. Now is the perfect time for covered entities and business associates to revisit the requirements under HIPAA and the steps they have taken to protect electronic health information.

---

[100] *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

ISSN 0747-8607