HIPAA AND THE INTERSECTION OF CYBERSECURITY IN HEALTHCARE

Authored by:
Marie Dieudonne, Principal, Divurgent

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has been around for a long time. The "1996" in the Act's name may give some the impression that it is antiquated—two decades is certainly considered eons in the cyber world in terms of the advancement of technology and the ability of bad actors to penetrate and exploit it. However, HIPAA has remained relevant as health information has migrated from paper to computers, mobile devices and even the cloud, and it has been continually updated and augmented.

The more electronic our healthcare information has become, the more cybersecurity has intersected with the healthcare sector and, therefore with HIPAA. As the threats to protected health information have evolved, so has HIPAA—a progression that has increased the level of complexity for those who must comply with the law or potentially face its penalties.

This whitepaper will address HIPAA and related legislation, who its regulations cover, and why compliance matters to individuals and organizations in healthcare. To know who is responsible and what they are responsible for in terms of compliance, it is first important to understand how HIPAA has evolved.

THE EVOLUTION OF HIPAA

Upon being enacted on August 21, 1996, the intent of HIPAA was to improve the portability and accountability of health insurance coverage for employees. Once HIPAA was signed into law, the Department of Health and Human Services (HHS) promulgated the *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), with a compliance date of April 14, 2003, and the *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule), with a compliance date of April 21, 2005.

The Privacy Rule establishes standards for the protection of protected health information held by covered entities and their business associates, and permits the use and disclosure of protected health information for patient care and other defined purposes. Under the Privacy Rule, patients are given certain rights with respect to their protected health information. Covered entities must comply with all requirements of the Privacy Rule, while business associates' responsibilities are somewhat more limited. The Privacy Rule contains important rights of individuals related to their PHI maintained by an entity.

The Security Rule establishes technical and non-technical safeguards that covered entities must implement to secure individuals' Personal Health Information (PHI) to ensure the protections contained in the Privacy Rule are met. It establishes security standards for protecting PHI that is held or transferred in electronic form. The safeguards that covered entities and their business associates must implement include, creating policies and procedures that demonstrate how they will comply with HIPAA, controlling physical access to data storage to prevent inappropriate

access, and protecting communications containing protected health information transmitted electronically over open networks.

Many covered entities initially failed to comply with the Privacy Rule and the Security Rule, resulting in HHS promulgating the Enforcement Rule, which went into effect in March 2006. Through this rule, HHS was given the ability to conduct investigations, assess civil monetary penalties, and provide opportunities for hearings and appeals.

In addition to protecting and securing protected health information, HIPAA had other objectives, which included combating waste, fraud and abuse in health insurance and healthcare delivery, and simplifying the administration of health insurance. Those simplification procedures became a means to encourage the healthcare industry to computerize patient medical records. This in particular, led to the enactment of the Health Information for Economic and Clinical Health Act (HITECH) in 2009, authorizing federal incentive payments to spur the adoption of electronic health record (EHR) systems.

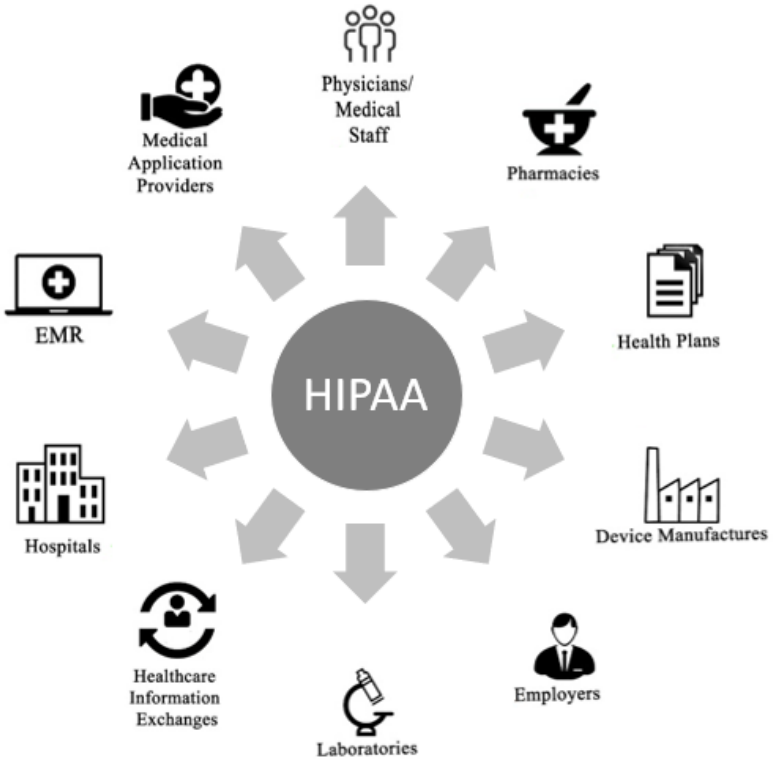
HITECH extended compliance with the Privacy Rule and the Security Rule to the business associates of covered entities, and introduced the Breach Notification Rule, which became effective on September 23, 2009. The Breach Notification Rule requires that all breaches of electronic PHI affecting more than 500 individuals be reported to the HHS Office of Civil Rights (OCR), while smaller breaches only need to be reported annually.

HITECH also strengthened enforcement of the Privacy Rule and Security Rule by increasing the maximum civil monetary penalty for violations of the same HIPAA requirement, establishing a tiered civil monetary penalty structure, and requiring HHS to investigate violations involving willful neglect. This act also required HHS to conduct periodic HIPAA audits to assess compliance by covered entities and business associates.

WHO IS RESPONSIBLE FOR HIPAA COMPLIANCE?

Because of its scope, HIPAA touches many entities and individuals, beyond those we have presented so far, who are involved directly or indirectly in the healthcare industry. Figure 1 below shows several other examples of those.

Figure 1: Entities and Individuals Touched by HIPAA



Before we go too far into explaining compliance and enforcement, we need to address to whom HIPAA applies. Two terms were repeated several times in the previous section: covered entities and business associates.

COVERED ENTITIES

Most organizations involved with providing healthcare or health insurance are considered "covered entities" with respect to HIPAA. These include health plans (e.g., self-insured plans, fully insured plans and health insurance companies) who provide "standard electronic transactions." These are defined in HIPAA as specific electronic transactions, including verifying patient eligibility, claims submission and remittance advice. Since most healthcare providers conduct these kinds of transactions regularly, they are considered covered entities.

BUSINESS ASSOCIATES

With the enactment of the HITECH Act, business associates also became directly liable for complying with some HIPAA provisions. Any vendor or independent contractor with access to protected health information in performing services for a covered entity is considered a "business associate" under HIPAA. Services that provide this kind of access are many, and include billing, practice management, data review, data analysis, data management, and utilization and quality review activities. People who provide administration and management services—such as accountants, attorneys and a range of consultants—and who receive protected health information, are also considered business associates subject to HIPAA.

Because of the HITECH Act, business associates must comply with some provisions of HIPAA, but they are doubly liable contractually because HIPAA requires covered entities to have business associate agreements (BAAs) with them. And covered entities must have these BAAs in place before disclosing any protected health information to them.

CONTINUING THE EVOLUTION

The Final Omnibus Rule of 2013, effective March 26, 2013, did not include any significant number of new requirements, but rather it specified certain criteria and amended provisions to provide clarity. For example, the Final Omnibus Rule of 2013 specified the encryption standards that must be applied to render electronic PHI unusable, undecipherable and unreadable. It also included amendments to account for technological advances, such as covering the use by healthcare professionals of mobile devices to access electronic protected health information.

Enforcement of HIPAA is divided among HHS, OCR, the Centers for Medicare and Medicaid Services (CMS), and the Department of Justice (DOJ). OCR enforces the Privacy Rule and Security Rule, and CMS enforces the electronic transactions and code sets provisions. Both OCR and CMS have the ability to refer any potential criminal violations to the DOJ, which enforces HIPAA's criminal sanctions. In addition, while states can promulgate and enforce their own medical privacy laws and regulations, as a result of HITECH, state attorneys are generally able to obtain damages in federal court on behalf of residents who are injured by a HIPAA privacy or security violation.

THE FTC HEALTH BREACH NOTIFICATION RULE

The FTC's Health Breach Notification Rule (FTC Breach Rule) applies to companies not covered by HIPAA, and requires notice in the event of any unauthorized acquisition of unsecured identifiable health information contained in a personal health record. It covers personal health records, which are defined as an electronic record of identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by, or primarily held by, an individual. The FTC Breach Rule applies to: vendors who offer or maintain personal health records; entities that interact with a vendor of personal health records by either offering products or services through the vendor's website or by accessing information in a personal health record or sending information to a personal health record; and third-party service providers that offer services involving the use, maintenance, disclosure or disposal of health information to vendors of personal health records or personal heath record-related entities.

Recognizing there could be some confusion over whether HIPAA or the FTC Breach Rule applies, given that some vendors of personal health records could also be business associates under HIPAA, the FTC issued some guidance on when the FTC Breach Notification Rule would apply in situations involving covered entities.

COMPLIANCE UNDER THE PRIVACY RULE

While the Security Rule has the most direct nexus to cybersecurity, understanding the Privacy Rule is critical to knowing when an unpermitted use or disclosure has occurred that may rise to the level of a breach. Individuals have certain rights, subject to limitations specified in the Privacy Rule, with respect to their protected health information. They are the rights to:

- Access or obtain a copy of protected health information
- Have their information amended for accuracy and completeness
- Obtain an "accounting," or a log, of disclosures of PHI
- Request confidentiality in communications
- Request a restriction on the use or disclosure of the information
- Receive a "Notice of Privacy Practices," outlining what the entity may do with the individual's protected health information

To comply with the Privacy Rule, covered entities must respond directly to the individuals asserting these rights, but business associates are not required to do so based on the regulations themselves. The most common arrangement is for the business associate to cooperate with the covered entity as the covered entity fulfills its responsibilities, and the details of such cooperation may be specified in a BAA. A BAA may also delegate the covered entity's duty to respond to the exercise of these rights, in which case the business associate is obligated to comply with the Privacy Rule's specifications in doing so. As stated above, the Privacy Rule also outlines what a covered entity can do with the protected health information it administers. Understanding when uses and disclosures are in violation of the Privacy Rule is critical to understanding when a breach has occurred, and consequently, if such potential breach warrants compliance with the notification requirements under HIPAA.

HIPAA restricts a covered entity's uses and disclosures of protected health information to only those uses or disclosures permitted or required by the Privacy Rule, or as explicitly authorized by the individual. There are many uses and disclosures permitted under the Privacy Rule for which no individual consent or authorization is required; primary among these are certain uses and disclosures for treatment, payment, and healthcare operations. These permitted uses and disclosures allow providers to exchange patient information to coordinate treatment, allow covered entities and billers to exchange patient information to facilitate payment, and allow covered entities to exchange patient information to accomplish various administrative tasks, such as consulting an attorney or business management services. Other examples of uses and disclosures not requiring individual consent or authorization include public policy-type disclosures such as those to aid law enforcement, for public health reporting, and pursuant to a court order.

Certain other uses and disclosures require the covered entity to provide the individual with the opportunity to accept or reject the covered entity's intended action. These include disclosures by facilities for directory listings, and disclosures to family members, friends, or anyone else involved in the individual's treatment or payment for treatment. The Privacy Rule outlines specific uses and disclosures requiring authorization, including the sale of protected health information. Ultimately, any uses and disclosures not otherwise allowed under the Privacy Rule would also require an individual to formally authorize the use or disclosure. HIPAA imposes strict requirements on what an authorization must contain, and any authorizations that fail to meet the requirements are considered invalid. In addition, even when covered entities are permitted to use and disclose protected health information, HIPAA requires that, in many cases, the covered entity only use or disclose the "minimum necessary" to accomplish the desired task.

Business associates are limited to the activities permitted by the applicable BAA. Although this permission typically is broad enough to permit a business associate to act in accordance with the demands of the arrangement or an underlying services agreement, business associates are bound to act in a manner permitted by the Privacy Rule. This means that business associates must also comply with the "minimum necessary" requirements.

Pursuant to the Breach Notification Rule, when there is a use or disclosure not permitted by the Privacy Rule, a breach is presumed to have occurred. Malware and other cybersecurity incidents that infiltrate the technological infrastructure of a covered entity or business associate are considered unpermitted disclosures and thus presumed breaches. Therefore, cyberattacks and security incidents implicate the Breach Notification Rule's processes for determining whether a breach has occurred that requires timely notification.

COMPLIANCE REQUIREMENTS FOR THE SECURITY RULE

The purpose of the Security Rule is to require covered entities and business associates to accomplish the following:

- Protect the "confidentiality, integrity, and availability of all electronic protected health information"
- Adopt measures to prevent potential risks to the data's "security or integrity"
- Seek to prevent any "reasonably anticipated" unpermitted uses or disclosures
- Ensure workforce members comply with all Security Rule requirements

Essentially, the Security Rule provides an outline of the minimum security requirements that a covered entity and a business associate must implement for all of their electronic protected health information.

While the Privacy Rule applies to all protected health information of a covered entity, the Security Rule is limited to that which is transmitted or maintained by electronic media, including computers, external hard drives, USB drives and other portable media, as well as internet and internal networks.

The Security Rule is broken down into three categories of requirements: administrative, physical, and technical safeguards. Most of these safeguards have implementation specifications, many of which are "required," which means that these specifications are mandatory, and some of which are "addressable," which does not exactly mean "optional." Instead, the Security Rule requires that the entity record why it is not able to implement the specific measure and describe what the entity has put in place to approximate the same level of protection that would have otherwise been afforded. The Rule requires that covered entities and business associates have a set of policies and procedures addressing each of these Security Rule safeguards and specifications.

The administrative safeguards are designed to ensure proper organizational oversight of the selection and implementation of the various security measures, including those related to personnel training and management. Such standards and implementation specifications include:

- Assigning a "security officer" designed to manage HIPAA security compliance
- Implementing processes for clearing incoming workforce members and terminating access of outgoing workforce members
- Categorizing and enforcing workforce members' access rights
- Training workforce members on security requirements
- Conducting a risk analysis and development of a risk management plan
- Implementing security incident identification and notification processes
- Developing contingency plans
- Executing business associate agreements, as appropriate
- Requiring appropriate password and other access procedures
- Providing security updates and using anti-malware and anti-virus software

The physical safeguards involve the physical protection of the facilities and equipment that maintain or transmit electronic protected health information, including:

- Implementing a security plan for facilities where electronic protected health information (ePHI) is maintained, accessed or transmitted
- Outlining appropriate workstation use, particularly with respect to the physical location of the workstation
- Tracking and recording the movement of mobile hardware and devices that have access to ePHI
- Implementing procedures for reusing and destroying workstations, media and the data itself
- Creating backup copies of all ePHI

The final standards are the technical safeguards, which focus on applying technology-based security measures to the entity's use of ePHI. These standards include:

- Encrypting data at rest and in transmission
- Implementing procedures to protect the integrity of the data to ensure that the data is not improperly modified or destroyed
- Auditing access and activity to ensure identification of any suspicious activity; and
- Verifying the identity of individuals seeking to access data.

The Security Rule has a direct nexus with cybersecurity for all entities subject to HIPAA, because, in total, the administrative, physical and technical safeguards cover incident prevention, identification, response and mitigation. OCR particularly emphasizes the security risk management requirements, including the performance of regular risk analyses and the development of a risk management plan. A risk analysis involves reviewing and determining the location and types of data, potential sources and likelihood of each risk, and potential effects and the magnitude of each risk if it does occur. Once the risks are fully evaluated, the risk management plan serves as a guide for the development of an entity's cybersecurity program and the adoption of security measures designed to account for or mitigate those identified risks. OCR considers these requirements fundamental to all other Security Rule measures, and, as such, these measures frequently are noted as an area of noncompliance in many recent OCR settlements.

With these mandatory and addressable security measures, entities may be concerned over what it takes to comply. However, looking at the regulations themselves, it is clear that the text does not include the exact details of what an organization must implement – there is no specific requirement for how long a password must be, or what type of anti-virus program must be included on every computer. This is because the Security Rule is specifically designed to be flexible so that different organizations can make the Rule's requirements work within their established structure. Specifically, the Rule requires that each organization, whether a business associate or a covered entity, take into account the following when evaluating what to implement for each measure:

- The "size, complexity, and capabilities" of the individual or organization
- The individual's or organization's "technical infrastructure, hardware, and software security capabilities"
- The costs of adopting measures to improve security; and
- The likelihood and magnitude of potential risks

OCR has published guidance on several important Security Rule topics that entities can utilize in developing their cybersecurity programs. For example, OCR has published an educational paper series that covers each set of standards as well as highlights the risk analysis and risk management plan requirements, which, as described above, are among the most important measures for entities to follow.

OCR also publishes a monthly cybersecurity newsletter that spotlights critical topics for consideration by its readers. Many of the OCR resources may be found by starting at the HHS HIPAA site at: https://www.hhs.gov/hipaa/.

In addition, the Office of the National Coordinator for Health Information Technology (ONC), another HHS subdivision, focuses specifically on health information technology topics. ONC has its own set of guidance materials available on its website, including those related to mobile devices and health information exchange. In conjunction with OCR, ONC has made available a Security Risk Assessment Tool to assist small and medium-sized providers in performing the mandatory risk analyses under the Security Rule. Using the tools provided by HHS may facilitate the development of an effective cybersecurity program in compliance with the Security Rule. ONC's privacy and security resources and tools may be accessed from this site: https://www.healthit.gov/topic/privacy-security-and-hipaa.

Perhaps most significant for the topic of HIPAA and cybersecurity is OCR's publication describing how ransomware attacks implicate HIPAA (Office for Civil Rights, 2016). Because of its publication year of 2016, the guidance document was likely released in response to a dramatic rise in ransomware attacks affecting healthcare providers and other companies in the healthcare industry. Per the guidance, OCR's position is that any ransomware attack is a "security incident," which is defined under the Security Rule as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system" (Office for Civil Rights, 2016, pp. 4-5).

Therefore, covered entities and business associates would need to look to their policies and procedures, and to trigger any security incident response procedures. For business associates, their obligations, at a minimum, are to report such security incidents to their covered entity clients or their higher-tier business associates, but their BAAs may delegate additional responsibilities for security incident response. With respect to whether these attacks would rise to the level of a breach, OCR has a more nuanced response. To determine whether a ransomware attack would constitute a "breach," OCR falls back on the fact-specific analysis specified in the Breach Notification Rule (Office for Civil Rights, 2016).

The boxed story on the following page shows examples of some of the recommended ransomware measures.

HIPAA and Ransomware

A ransomware attack qualifies as a HIPAA breach and so must be reported if 500 or more records are affected. As such, the HIPAA Security Rule requires that healthcare entities (and their vendors) implement security measures to help prevent the introduction of ransomware, as well as respond to and recover from a ransomware attack (Office for Civil Rights, 2016). Specifically, they should:

- Conduct a risk analysis to identify threats and vulnerabilities to ePHI, and establish a plan to mitigate or remediate those identified risks.
- Implement procedures to safeguard against malicious software.
- Train authorized users on detecting malicious software and reporting such detections.
- Limit access to ePHI to only those persons or software programs requiring access.
- Maintain an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations.
- Maintain frequent backups and ensure the ability to recover data from backups through periodic test restorations. Because some ransomware variants have been known to remove or otherwise disrupt online backups, entities should consider maintaining backups offline and unavailable from their networks.

If you are hit with ransomware, implement your security-response and continuity plans, and contact the FBI before you agree to pay any ransom.

OCR also promotes use of the various white papers from the National Institute of Standards and Technology (NIST) for the development of one's compliance program. NIST, a part of the Department of Commerce, develops, tests and promotes standards and measurements for the benefit of various industries. Among NIST's many projects is the Cybersecurity Framework, which provides a guide for businesses seeking to adopt and implement a robust cybersecurity program (NIST, 2018). Focused on risk management, the "core" of the Framework focuses on five elements: identify, protect, detect, respond, and recover. NIST and HHS have jointly published a "crosswalk" document that links the Cybersecurity Framework to the HIPAA Security Rule requirements to ensure that, in keeping with NIST's best practices, entities are also aware of their compliance responsibilities (Office for Civil Rights, 2016a).

OCR further points to certain of NIST's "Special Publication" guidance documents for more information on discrete topics within the cybersecurity world, including encryption. Essentially, NIST guidance documents can serve to provide more details on best practices for certain specific security measures and the development of an effective and compliant cybersecurity program.

COMPLIANCE UNDER THE BREACH NOTIFICATION RULE

In response to the HITECH Act, HHS imposed additional requirements on covered entities and business associates that experience a breach of protected health information. A "breach," as defined by the HIPAA regulations, is any use or disclosure of unsecured protected health information, contrary to the Privacy Rule, that compromises the privacy and security of that information, subject to a few narrow exceptions. "Unsecured" means that the information "has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by [HHS] guidance." For electronic data, this means encryption, and HHS points to several NIST publications for valid encryption processes (HHS, 2013). Note that OCR warns in its ransomware guidance that encryption is only effective as a method of preventing a breach when it truly is rendering the data unreadable or unusable; for example, it points to the example of full disk encryption on a computer as not "securing" data when the computer is in use (OCR, 2016).

Where a covered entity experiences an unauthorized use or disclosure of unsecured health data, a breach is presumed unless the covered entity assesses the disclosure and documents that there is a low risk that the protected health information was compromised. The risk assessment must evaluate at a minimum four specific factors:

- the type and volume of protected health information involved
- the identity of the person or entity that impermissibly used or received the data
- the likelihood that the information was "actually acquired or viewed"
- the extent of any mitigation efforts

If the covered entity determined that there is more than a low risk, the covered entity must move quickly to make the required notifications. If notification is required based on the risk assessment, then the covered entity (or business associate, if delegated in the BAA), must meet the following requirements:

Who	When	What
Individuals affected or believed to be affected	As soon as possible, but no later than 60 days following the breach's discovery	Notification letter (or email, if consent for electronic communications obtained) If more than 10 individuals cannot be reached by written notice, substitute notice in the form of either posting to the entity's website or press release to the media and use of a toll-free phone line
HHS	For breaches affecting >500 individuals, as soon as possible, but no later than 60 days following the breach's discovery For breaches affecting <500 individuals, track all "smaller" breaches and notify HHS of all such breaches within 60 days following the end of the calendar year	Online reporting form available on HHS' website
Media	For breaches affecting >500 individuals in a state or jurisdiction, as soon as possible, but no later than 60 days following the breach's discovery	To "prominent media outlets," typically by press release, containing the same information required to be in the notice to individuals

The Security Rule itself only requires business associates to notify and cooperate with covered entities with respect to breaches caused by or occurring at the business associate (or a subcontractor, as reported by that entity). Covered entities may negotiate for stronger breach response provisions, sometimes providing stricter timelines, passing down the financial liability for breach notification, or requiring business associates to perform the notifications on the covered entity's behalf. Business associates experiencing breaches must look to each agreement to know how to respond in the event of a breach.

Breaches happen, whether "high-tech" or "low-tech." For those that are "high-tech," a robust cybersecurity program that is compliant with the Security Rule ideally would help an entity catch, respond to, and mitigate that breach. As stated above, OCR believes that cyberattacks are security incidents, which should trigger an analysis into whether a breach occurred, and if notification is necessary (OCR, 2016). Failure to do so in compliance with the Breach Notification Rule can lead to enforcement issues.

WHY IS COMPLIANCE IMPORTANT?

As mentioned before, the HHS Office of Civil Rights administers and enforces HIPAA regulations. Many see the regulations as onerous. In a Politico blog in early March, OCR Director Roger Servierno was quoted as saying at a meeting at the HIMSS 2018 conference that his office was seeing "if there are deregulatory opportunities, and that includes our HIPAA regulations." (Tahir, 2018).

While this quote might give OCR watchers a glimmer of hope of some kind of relief, the current reality is that HIPAA compliance is not optional for many individuals and organizations in the healthcare industry and the people who do business with them.
As seen above, the Privacy, Security, and Breach Notification Rules provide a long list of requirements that constitute HIPAA compliance. OCR identifies the following as its most commonly investigated issues:

- Uses and disclosures made in violation of the Privacy Rule
- Lack of safeguards for protected health information (not just electronically held data)
- Failure to comply with an individual's right to access their own information
- Failure to comply with the "minimum necessary" requirements
- Inadequate administrative safeguards under the Security Rule

Further, the settlements published by OCR provide further insight into the compliance issues frequently uncovered by OCR. For example, in 2016, the most common issues that entities had when subjected to investigation by OCR were as follows:

- Failure to conduct a complete and comprehensive risk analysis;
- Failure to enter into a Business Associate Agreement before disclosure;
- Failure to have or failure to implement Security Rule policies and procedures
- Failure to put in place appropriate risk management procedures and measures designed to prevent security incidents or breaches of electronic protected health information

Compliance with these HIPAA requirements is important for many reasons, not the least of which is the creation of a base level protection for patient health information. However, another significant motivation is the potential financial impact of noncompliance.

OCR enforcement activities can begin a variety of ways, including complaints, audits, breach notifications, and referrals. Media reports of breaches or other HIPAA violations can also pique OCR's interest and result in an inquiry from the agency. Many complaints are filtered out early on due to lack of jurisdiction, expired filing deadline, or lack of violation. For those that proceed to a compliance review, many more result in the provision of technical assistance (e.g., guidance on how to remedy noncompliance), or a requirement for corrective action. A few can result in more serious consequences, such as civil monetary penalties and resolution agreements.

Simply put, HIPAA violations can result in serious, expensive penalties:

Type of Violation (Mental State)	Penalty for Single Violation
Did Not Know	$100-$50,000
Reasonable Cause	$1,000-$50,000
Willful neglect – Corrected	$10,000-$50,000
Willful neglect – Uncorrected	$50,000

For multiple violations of the same HIPAA provision in the same year, the penalties can reach as high as the maximum of $1.5 million, and multiple violations of multiple provisions of HIPAA can result in penalties well over that. As of January 31, 2018, the highest settlement to date is $5.55 million, with the total number of amounts collected via settlements or civil monetary penalties totaling more than $75 million. In 2016, OCR had one of its most active years for settlements, with 12 settlements and one civil monetary penalty, seven of which resulted in payments of over $1 million each. OCR also enters into Resolution Agreements pursuant to these settlements, which in addition to including any settled amount, impose corrective action plans that provide for OCR oversight over the implementation of policies and procedures and other measures to resolve any HIPAA noncompliance. (OCR, 2018)

In addition to these financial penalties, OCR may also refer cases to the Department of Justice for criminal prosecution; as of December 1, 2017, it has done so over 600 times. Further, many may fail to realize that, although OCR is the federal enforcement entity with respect to HIPAA (and sometimes the DOJ), states' attorneys general can bring their own actions to protect the interests of their citizens.

Enforcement activity has certainly increased in recent years, with OCR reaching more settlements with covered entities (and the first business associate in 2016) and OCR's implementation of the next phase of its audit program. Tracking enforcement activity can provide valuable insight into OCR's areas of focus and inform each entity's privacy and security compliance programs.

Covered entities and business associates should therefore consider HIPAA in tandem with the development of their cybersecurity programs, to ensure that they embrace compliance with the Privacy, Security, and Breach Notification Rules, while avoiding being the subject of OCR's enforcement actions.

ABOUT THE AUTHOR

Marie Dieudonne, Principal

In her role as Principal, Marie leads Divurgent's Population Health and Value-based Care programs, pulling from her more than 20 years' of experience collaborating with individuals, leading teams, and transforming organizations, helping them clarify goals and solving problems with a "let's get it done" attitude. Her experience ranges from engineering, line management, leadership development, business development, project and program management, product development, portfolio management, strategic planning, and Lean Six Sigma process facilitation. She has worked with both global companies and startups, in the chemical/plastic, finance, high-tech, software, and healthcare industries.

Passionate about changes on the horizon, Marie's work is focused on transitioning complex healthcare organizations from volume-based payment structures to value-based care delivery, aligning physicians and hospitals with measurable cost, quality, and outcomes solutions. She applies Patient Access strategies and meaningful process improvement solutions and best practices to help clients align organization, business, and technical goals to maximize their resources and prepare for the future of payment and care.

Most recently, Marie worked as a healthcare consultant with a focus on enabling the use of available data with analytics; learning and creating solutions for population health initiatives and effective care management delivery; developing and implementing the right technology with good process and compliant practices and creating the measurement systems supporting quality and business results. Prior to becoming an independent healthcare consultant, Marie worked with a national healthcare payer, a TPA and a consumer wellness company. Marie spent more than 12 years with General Electric Co, gaining extensive experience and practice in several business units including GE Plastics, GE Appliance/Lighting, GE Capital, and GE Healthcare.

Email | LinkedIn

REFERENCES

Department of Health and Human Services. (2013). Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals. available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

National Institute for Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework/framework.

Office for Civil Rights. (2010) Guidance on Risk Analysis Requirements under the HIPAA Security Rule. Retrieved at https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Office for Civil Rights. (2016) Fact Sheet: Ransomware and HIPAA. Retrieved from https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Office for Civil Rights. (2016a). HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Retrieved from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es

Office for Civil Rights. (2018, January 31). Enforcement Highlights. Available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html?language=es

Tahir, D. (2018, March 7). Trump Administration at HIMSS [Web blog]. Morning eHealth. Politico. Available at https://www.politico.com/newsletters/morning-ehealth/2018/03/07/trump-administration-at-himss-124713