# Back to the Basics: HIPAA Compliance 101

*by* **Marissa Rufo** | *MZQ Consulting, LLC*

With a record high number of health care security breaches reported in 2023 to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), it should come as no surprise that cybersecurity and the Health Insurance Portability and Accountability Act (HIPAA) have become hot topics for the health insurance industry in 2024. While this is not a completely new problem, since security breaches have increased year over year for about a decade, it seems that the trend toward using technology to aid in health insurance administration may come with some pros and some even more costly cons.

In 2023, more than 540 organizations reported HIPAA breaches that affected approximately 112 million individuals across the country. Many of these HIPAA security incidents involved third-party vendors that handled HIPAA-protected information.[1] HIPAA garners most of its public attention in relation to how individuals' private health information is handled in a medical provider setting. But the law also applies to health insurance administration and the various actors involved in the process—a compliance obligation that many in the health insurance industry may have forgotten in the midst of what feels like an ever-expanding list of additional compliance rules for health plans.

The recent trend in HIPAA breaches emphasizes the importance of revisiting (1) the basics of HIPAA compliance, (2) what health plan advisors or sponsors can do to mitigate risk when implementing new technologies and handling HIPAA-related information, and (3) what this all means for health plan fiduciaries.

## What Is HIPAA?

HIPAA was enacted to create uniform standards for electronic health care transactions and security when handling protected health information (PHI). The law—much like the technology that spurred its creation—has evolved in the decades since its inception, with requirements added by the subsequent enactment of the Privacy Rule, the Security Rule, and the Health Information Technology for Economic and Clinical Health Act (HITECH).

For health plan sponsors and administrators, it is particularly important to define and understand to whom and to

## AT A GLANCE

- In 2023, more than 540 organizations reported breaches of the Health Insurance Portability and Accountability Act (HIPAA) that affected approximately 112 million individuals across the country. Hacking-related data breaches increased 239% between January 2018 and September 2023.
- The HIPAA Privacy Rule governs how health plans allow participants to access their protected health information (PHI), while the HIPAA Security Rule sets national standards for how plans must protect PHI and keep it confidential.
- Strategies that health plans should consider to help them remain in compliance with HIPAA include knowing the basics, building out HIPAA policies and procedures, using multifactor authentication, obscuring PHI and ePHI, and running penetration testing.

what information HIPAA applies. This will help these entities strategize to ensure that the data related to their health plan does not fall victim to a HIPAA breach.

The following is an outline of the basics of HIPAA.

### *The Privacy Rule*

The HIPAA Privacy Rule was issued in December 2000 and laid a framework of rules regarding the access of PHI for covered entities, including health plans. Health plans must allow plan participants access to their PHI upon their request as well as transmit such information to any other identified entities. Further, they must ensure that information transmittal—whether on paper or electronic—is done in a protected manner.

### *What Are PHI and ePHI?*

HIPAA and its regulatory additions were designed to keep PHI from falling into the wrong hands while a health plan is being administered. Not every piece of information collected in health plan administration is considered PHI. The test for what constitutes PHI can be broken down into two parts:

1. Is the information individually identifiable? *Individually identifiable* means that the information could be traced back to a particular person and likely contains demographic data related to an individual's past, present or future health care, medical conditions, etc. This information does not have to directly name or identify an individual to meet the definition of individually identifiable information. For example, if information referred to an individual under the group health plan who suffered a catastrophic health event in the month of January of that year, and there is clearly only one employee who would fit that definition at the organizational level, that information may be categorized as individually identifiable.
2. Is the individually identifiable health information in the possession of a covered entity? Health plans—whether individual or group plans—are considered covered entities, including major medical, dental, vision, prescription drugs and supplemental benefits.

The vendors involved in plan administration as well as the plan sponsors should be aware of the HIPAA rules and prioritize the security of plan participant information.

*Electronic PHI (ePHI)* is PHI that is created, stored, transmitted or received in electronic format or media. Understanding what constitutes ePHI is important when strategizing and implementing security standards for health plan information to comply with the HIPAA Security Rule. While all PHI, whether in electronic format or paper, must be held to the same security standards, ePHI and the evolution of technology in health plan administration have created a different level of potential risk for organizations and plan sponsors.

### *The Security Rule*

The HIPAA Security Rule was enacted in February 2003 and set national standards for how to protect and keep confidential PHI and ePHI. To remain in compliance with HIPAA, health plans and their business associates must implement a HIPAA compliance process and associated procedures within their organization that ensures that the storage and transmittal of PHI and ePHI is done safely.

The Security Rule was originally drafted to allow for flexibility in business decisions for health plans as they adopt and implement a variety of technologies. While innovation in health plan administration is always welcome, the rule outlines the importance of not innovating yourself out of compliance in the process.

### *HITECH, HIPAA's Cousin*

HITECH was enacted in 2009 and expands on the HIPAA Privacy and Security Rules. HITECH provides direct regulation of business associates (and identifies them as being subject to the rules of HIPAA) and increases the requirements for responding to breaches. Most notably, HITECH also expands on the governmental authority to enforce these compliance regulations and access civil penalties when organizations are not in compliance.

### *What Is a Business Associate?*

A *business associate* is a person and/or organization outside the covered entity that performs certain functions on behalf of the health plan that may involve the use or disclosure of PHI/ePHI. Common functions of business associates include claims processing, plan data analysis, utilization reviews and reporting, and plan billing.

When a plan functioning as a covered entity uses a contractor to perform business associate services or activities, it must have certain protections in place outlined in a business associate agreement. While contractual in nature, this agreement must outline the use and disclosure of PHI and the safety procedures utilized by both parties in the agreement, including any data information technology utilized, data storage operations and rules, and what each party should do in the event of a breach.

## HIPAA Breaches and Notification

The HIPAA Breach Notification Rule outlines the process of reporting HIPAA breaches to HHS and/or the Federal Trade Commission (FTC) where applicable. A *breach* is defined as any impermissible use or disclosure of PHI/ePHI that compromises the security or privacy of the information accessed.[2]

Not all HIPAA breaches are created equal though, and some exceptions apply for reporting a breach. The HIPAA breach notification exceptions are as follows.

1. The access or use was made in good faith and within the scope of authority of the accessing individual.
2. An inadvertent disclosure happened between two authorized persons, and/or
3. There was a good faith belief that the unauthorized personnel who received the information would not have been able to retain the information.

Assuming that the breach does not fall within the exceptions mentioned, the covered entity must notify the affected individuals, the HHS secretary and (in some cases) the public media after it is discovered. The requirements of those rules vary.

The rule for notifying affected plan participant individuals requires that notices be furnished whenever the discovery of a breach is made. The HIPAA Breach Notification Rule for affected individuals also contains specific timing requirements to remain compliant. The rule for notifying the HHS secretary applies to HIPAA breaches that affect 500 or more individuals and includes notification timing requirements to remain compliant. Lastly, the rule for public media notification for HIPAA breaches involves a breach that consists of 500 or more affected individuals that reside within the same state or jurisdiction. The last scenario, as one can imagine, would be the worst case because the party that suffered the breach must notify the media and suffer the consequence of the bad publicity often associated with it.

## HIPAA and Cybersecurity

Throughout the 2000s, innovation and technological development have shaped how industries, including the health insurance industry, provide services for their customers. While embracing technology and creating patient-facing online capabilities may be a consumer-friendly solution to improving services, it may also be a sitting duck for cyberattacks and HIPAA breaches.

In 2023, the majority of breaches publicly listed by HHS OCR were reported by health care providers, with 358 incidents affecting 35 million individuals. Business associates reported 112 incidents affecting 59 million individuals, and health plans reported 82 incidents affecting 15 million individuals.

OCR reported a 239% increase in hacking-related data breaches between January 2018 and September 2023.[3] A trend toward employing digital recordkeeping and cloud-based services to help vendors and plan sponsors administer health plans, while efficient for customer service, has also left them vulnerable to hackers seeking PHI/ePHI. Prior to the health technology boom that has been taking over the industry, individuals' PHI was more likely to be kept on paper in one location or stored locally on an electronic system that would require physically stealing equipment to retrieve it.

Compared with breaches attributed to theft and unauthorized access/disclosure, the hacking/IT incidents account for about 60-80% of all reported HIPAA breaches annually. As technology evolves and companies no longer exist in singular brick-and-mortar environments, data storage and management has adapted as well to support organizations in web-based or hybrid working environments. The "cloud," while a fun word used to refer to a system of integrated data management across systems, is also full of stormy possibilities if it is not managed correctly. Much like the clouds in our sky, they are both helpful and harmful at times. Cloud data management is a phenomenal resource to centralize data management and improve accessibility for individuals at a company, but without proper security measures, it can also increase access points for bad actors.

To underscore the potential vulnerability of this tool, many of the recent hacking-related breaches come in the form of ransomware attacks. As the name suggests, ransomware is a type of malware or malicious code that hackers plant to hold the victim's data and/or device "hostage" and then require a ransom to regain access to it. As protections have improved, hackers have refined their strategies; attacks with ransomware now often also target known backup servers as well so the victim organization cannot even restore its data unless it complies with the hacker's demands.

Even entities that protect themselves can be impacted if third-party vendors are attacked. For example, in 2023, NationsBenefits Holdings, LLC, which provides administrative services to several well-known insurers, suffered a data breach when cybercriminals attacked a third-party data vendor. The breach resulted in unauthorized access to individuals' PHI. While this is an example of a severe HIPAA breach, there are some positives to glean from the incident. NationsBenefits' team was able to identify a potential breach prior to receiving notification from its vendor, thanks to security controls already in place to prevent potential breaches from occurring and continuing. The company then acted swiftly in notifying its data vendor and began its own internal investigation. Since the breach, NationsBenefits has stated that it has strengthened its security measures, taken its managed file transfer (MFT) servers permanently offline and is no longer relying on the vendor to provide file transfer solutions.

Using this example as a test case, one can see how quickly the domino effect of a cyberattack and HIPAA breach can affect the various group health plan actors. Even though NationsBenefits had security protocols in place for itself, it still suffered a substantial HIPAA breach. How does this relate to compliance measures? The answer is simpler than one might imagine. With proper HIPAA compliance in place, the negative impact of events like this hack can be vastly lessened, and the steps to prevent them from happening are not as difficult as one might think. For more information, see the "Five Tips" section beginning on page 16.

## Enforcement

The enforcement of HIPAA compliance is done in a few different ways that span from government actions to private actions of plan participants. HIPAA enforcement at the federal government level is accomplished through the HHS OCR office or through the Centers for Medicare & Medicaid Services (CMS) National Standards Group (NSG).

### *Office for Civil Rights*

OCR has the primary authority to investigate and enforce the HIPAA Privacy and Security Rules. The agency's investigations start in one of two ways—Either a breach was so large that a report to HHS is required, or someone may report an entity to HHS for potential HIPAA violations. OCR prioritizes HIPAA complaints how one might imagine. Large breach notifications are an immediate red flag to investigate what has happened and how to take corrective action. Anonymous reports to OCR may result in an investigation and enforcement action, or they may be resolved before OCR initiates an investigation at all.

### *CMS NSG*

The CMS NSG compliance review program was established in 2019 to aid in the enforcement of HIPAA compliance on behalf of HHS. The program focuses on a select number of randomized audits of health plans and clearinghouses. Health plans chosen to participate in these compliance audits will receive the findings of their audit. If noncompliance issues arise, these plans will be referred to HHS for guidance and potentially corrective action plans to remedy the issues.

The CMS NSG office publishes its annual findings, including trends in HIPAA violations based on that year's audits, as well as educational material on how to better achieve HIPAA compliance.[4]

### *Enforcement Penalties*

When a HIPAA violation is found and confirmed, the result from an enforcement perspective will be the same. The plan sponsor and/or breach party will be responsible for civil penalties assessed by HHS as well as the potential private action rights and monetary penalties that may be the result of a lawsuit related to the HIPAA breach. These HIPAA breach incidents can become very costly very quickly for the noncompliant party. Further, it is important to keep in mind that violation penalties are based on severity of the incident and culpability of the breaching party (e.g., whether it knew, should have known or were just negligent in the incident).

The following real-world examples illustrate how these scenarios play out and how costly HIPAA breaches can become.

### Anthem, Inc.[5]

In 2015, health insurer Anthem filed a report with the OCR detailing a breach of its IT system that resulted in hackers stealing the ePHI of almost 79 million individuals over the span of approximately two months. The breach resulted in a class action lawsuit settlement of $115 million to the victims of the breach and a $16 million settlement with OCR with the promise of a corrective action plan. OCR's investigation revealed not only impermissible disclosures of ePHI, but that Anthem failed to conduct a risk analysis, had insufficient procedures in place and generally failed to create a compliant system with adequate security in place for its ePHI.

### True Health New Mexico Inc.[6]

In 2021, True Health New Mexico, a New Mexico-based health insurance provider, discovered and reported a breach that affected almost 63,000 members of its health plans. During the investigation, it was discovered that unauthorized individuals accessed the company's network and used ransomware to access the ePHI of the identified members. A class action lawsuit settlement was reached in which potentially 62,982 True Health patients could collect up to $330 million in damages.

### Excellus Health Plan, Inc.[7]

In 2015, Excellus Health Plan reported a breach that was later discovered to have spanned from December 23, 2013 through May 11, 2015. OCR's investigation revealed that the breach consisted of access to around seven million health plan members and approximately 2.5 million members of the plan's subsidiaries. According to an HHS press release, cyberattackers gained unauthorized access to the plan's IT systems and installed malware and conducted reconnaissance activities. The OCR investigation revealed that the health plan was potentially noncompliant with five major standards of the HIPAA rules, was lacking in the technical policies and procedures necessary to keep its ePHI safe, and most notably failed to conduct an organization-wide risk analysis. The incident resulted in approximately $5.1 million in penalties to settle the HIPAA violation and a class action lawsuit that resulted in a settlement for approximately $4.35 million after about a decade of legal battles surrounding it.[8]

## Five Tips for How to Get Hip With HIPAA

The following are best practices and simple ways to assess a plan's current HIPAA compliance and risks.

### *1. Start With the Basics (Know the Rules)!*

Plan sponsors should start by getting familiar with HIPAA's rules and requirements. To do so, they should make sure that their team goes through basic HIPAA training. HIPAA training will provide a more in-depth education on the Privacy and Security Rules as well as guidance on building the framework for the company's HIPAA compliance strategy, including who on the team will be directly involved in the day-to-day monitoring of systems and information. In addition, it is important to note that someone in the organization should be designated as the HIPAA compliance officer and/or the primary personnel in their organizational role in charge of HIPAA compliance.

This person should oversee ongoing HIPAA compliance, monitor organizational security and be the individual to whom potential breaches are reported. Having proper security measures set up is of no use if there is no one making sure they remain in place. Even the best system is susceptible to hacks, so organizations need to have identified personnel ready to respond when an incident occurs.

### *2. Build Out HIPAA Policies and Procedures*

If they have not already, those involved in the administration of a health plan will need to create the internal processes and procedures the plan follows to remain in compliance with HIPAA.

These may include strategies such as:

- **Monitoring and reporting PHI and ePHI access:** Health plans should track who sees PHI and ePHI (examples of which include claims information as well as plan participant eligibility and enrollment) and track when they see it on their company devices and access points. They should also run quarterly reports on all access activity related to PHI/ePHI—This will be very helpful if a breach occurs.
- **Ensuring that business associate agreements (BAAs) are in place:** Does the organization have written BAAs in place where necessary, including between other business associates and subcontractors? While not related to IT security measures, having BAAs in place is of utmost importance when outlining the roles of vendors and plan sponsors and the liability owed to each if there were to be a HIPAA breach occurence.
- **Utilizing device encryption software:** Device encryption runs in the background of a system to help protect plan data. A commonly used system is BitLocker, which is available as a Windows feature on Windows-enabled devices.[9] These types of internal security measures are essential to preventing unwanted parties from accessing information related to health plans and participants.
- **Using a password management system:** These not only help individuals within the team store all their passwords securely but also allow for new and safer passwords to be generated at regular intervals, making it harder for hackers to gain access. As hackers become more sophisticated, the tools available to combat them do as well. Plans should consider using a password management system that both ensures safer passwords and tracks out of the ordinary activity in password inputs.

### *3. Utilize Multifactor Authentication*

Traditionally, multifactor authentication (MFA) was done with just a username and password; however, cyberattacks have become more sophisticated and this strategy is no longer enough to keep ePHI and PHI safe. Sometimes referred to as two-step verification, MFA now incorporates an application or website to verify the user's identity further, with items such as a time-sensitive personal identification number (PIN), passcode, facial recognition, etc. Many online banking platforms and financial sites have already begun using these types of security requirements for account access.

AUTHOR

**Marissa Rufo** is a compliance advisor, regulatory affairs, and subject matter expert at MZQ Consulting, LLC, a benefits compliance and Affordable Care Act reporting firm in Pikesville, Maryland. Her legal background focused on litigation including broad civil litigation, personal injury, employment/union contracts as well as civil and criminal tax controversy. Rufo earned her B.A. degree from the University of Maryland. She also completed a dual degree program, earning J.D. and M.B.A. degrees from the University of Baltimore School of Law and School of Business, respectively.

### *4. Obscure PHI and ePHI*

There are technical strategies available to make it more difficult for hackers to access the PHI within a system, such as obscuring PHI. Think of this like making the hackers unlock a box, locked inside another box, all with different passcodes to get in. The more layers of protection you force outside individuals to get through to access the PHI, the safer it will be. In 2023, a significant number of large, health care-related security breaches were the result of hackers gaining access to the key to a commonly used data file transfer service named MOVEit. Once the hackers figured out the flaw within the system, they were able to hack millions of instances of PHI across numerous systems, the impact of which is not even fully understood yet.

As the investigation into the MOVEit breach incident continues, some trends have been discovered. In particular, many of the individuals affected were using the MOVEit file transfer services with minimal to no additional protections, which enabled the hackers to easily access additional pieces of their systems through that one entry point. And while no one can create a system that is 100% secure from any HIPAA breach/hacking incident, organizations can take steps to protect the PHI within their systems, even when a hacker gains access to a portion of it. Obscuring PHI and not allowing it to linger in places such as file transfer services or web-based servers outside the organization can greatly improve the chances that hackers don't gain access to unprotected PHI (or, if they do, it is only a small recently transferred PHI data set).[10]

### *5. Run Penetration Testing*

Penetration testing, sometimes referred to as "pen testing," is a security exercise in which a cybersecurity expert attempts to find and exploit vulnerabilities in IT systems. Imagine hiring a hitman, except their "hit" is the plan's own technical systems. If they are successful in their efforts, then the plan knows where the problems lie within the system. There are multiple types of penetration testing available and numerous companies that specialize in this security testing method.[11]

## Closing Thoughts

HIPAA compliance has grown to be a daunting task for many organizations to meet. The complexity of the rules pertaining to PHI/ePHI, as well as the speed at which technology has developed, combined with the lack of discussion around HIPAA compliance in recent years has left many organizations at risk of a security incident. However, the Departments (i.e., HHS, CMS) are making HIPAA compliance and enforcement a priority in 2024.

With various ways to get hung up on a HIPAA compliance issue, it is important to note that there is help available to take steps in the right direction. The Departments have released various educational resources online in the form of self-help tools, as well as annual reporting numbers of HIPAA breaches and investigations, which are publicly available for organizations to study. Many compliance and technology resources are available to test systems, train individuals in HIPAA compliance, and help you strategize compliance efforts if a plan ends up having a HIPAA breach incident.

In a world full of new compliance obligations, plan sponsors should stay diligent and go back to the basics. Regular training, continued education and even taking the time to read articles such as this one will help keep plan sponsors a step ahead!

## Endnotes

1. https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches.
2. www.hhs.gov/hipaa/for-professionals/breach-notification/index.html).
3. www.hipaajournal.com/healthcare-data-breach-statistics.
4. https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/enforcement/compliance-review-program.
5. www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach.
6. www.hipaajournal.com/true-health-new-mexico-proposes-settlement-to-resolve-class-action-data-breach-lawsuit.
7. www.hipaajournal.com/excellus-health-plan-settles-hipaa-violation-case-and-pays-5-1-million-penalty.
8. https://thnmsettlement.com/Content/Documents/Motion%20for%20Final%20Approval.pdf.
9. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/#device-encryption.
10. https://www.safebreach.com/blog/moveit-vulnerability-a-painful-reminder-that-threat-actors-arent-the-only-ones-responsible-for-a-data-breach.
11. hwww.cloudflare.com/learning/security/glossary/what-is-penetration-testing.

**International Society of Certified Employee Benefit Specialists**

Reprinted from the Third Quarter 2024 issue of *BENEFITS QUARTERLY*, published by the International Society of Certified Employee Benefit Specialists. With the exception of official Society announcements, the opinions given in articles are those of the authors. The International Society of Certified Employee Benefit Specialists disclaims responsibility for views expressed and statements made in articles published. No further transmission or electronic distribution of this material is permitted without permission. Subscription information can be found at iscebs.org.

pdf/724