Articles + Publications | June 4, 2025

3 Takeaways From Recent Cyberattacks On Healthcare Cos.

WRITTEN BY

Sadia Mirza | Brent T. Hoard | Kaitlin J. Clemens

Significant data breaches have affected major players in the healthcare industry in the last year, with the methods of attack being as diverse as the affected entities themselves.

They included large-scale ransomware assaults directly on healthcare providers like Acadian Ambulance Service and on third-party service providers, such as Concentra Health Services' breach at its third-party transcription service vendor.

The pattern of large-scale data breaches has persisted this year. For instance, Frederick Health Medical Group disclosed in January that it experienced a cyberattack, which may have exposed the protected health information, or PHI, of approximately over 900,000 patients.

Recent reports highlight that these incidents are not diminishing anytime soon. System intrusion, including ransomware is the top cause of breaches in the healthcare sector, which has seen a rise in incidents and breaches over the past year, according to Verizon Business.[1]

Threat actors are not only targeting healthcare entities directly, but the trends show threat actors increasingly targeting healthcare service providers such as radiology service providers, IT providers, medical transportation firms and pharmacies. Altogether, the average cost of a data breach in the healthcare industry reached $9.77 million dollars and topped the list for costliest industry for breaches, according to an IBM report.[2]

Together, incidents from the last year and a half have led to the unauthorized access or theft of healthcare information for millions of patients. The upward trend in costs, styles of attacks and entities attacked highlighted the critical importance of proactive planning to help organizations withstand the operational, legal and reputational turmoil that can follow a data breach.

Reflecting on the responses to these large-scale incidents and considering the direction in which these attacks are evolving reveals three essential strategies that healthcare organizations can adopt to bolster their resilience against future cybersecurity threats: proactively preparing for operational disruptions; clearly defining roles and responsibilities related to data management and incident response; and engaging early with regulatory bodies to better position the organization and those potentially affected by the incident.

A Couple Refreshers

Ransomware and Data Theft

Ransomware and data theft remain significant threats to healthcare entities. Ransomware threat actors sometimes employ a double-extortion model. When this happens, they initially infiltrate a victim's environment to locate and remove data from the victim's systems. To compound the damage, they then deploy a ransomware payload, encrypting the environment and disabling at least some of the organization's systems.

At times, the threat actor may leave a ransom note demanding payment to either decrypt the environment or prevent the publication or sale of the stolen data. This business model primarily affects organizations by disrupting business operations, potentially triggering legal notification obligations and causing a PR crisis.

Data thefts can also occur without ransomware. In such cases, while there is usually less operational impact or business downtime, healthcare entities still face legal and reputational repercussions.

While many attacks are opportunistic, some threat actors are now specifically targeting the healthcare industry due to the critical nature of their operations and the potential sensitivity of the data that they hold. Greater operational disruption and larger quantities of stolen sensitive data can, in theory, lead to higher payouts for these malicious actors.

Over the past year, the healthcare industry experienced significant cyberattacks. Acadian Ambulance Service, which provides air and ground ambulance services, faced a cyberattack that exposed the PHI of approximately 2.8 million individuals. This attack was allegedly carried out by a cybercriminal group known for targeting healthcare organizations.

Additionally, Concentra Inc., a Texas-based physical and occupational health provider, confirmed in 2024 that almost 4 million patients were affected by a breach at its transcription service provider.

U.S. Breach Notification Law

When a healthcare entity suffers a data breach, the entity may face notification obligations under both state data breach notification statutes and the Health Insurance Portability and Accountability Act. Other incidents may sometimes trigger notification obligations imposed by international breach notification laws, to the extent international residents are involved.

Each state in the U.S. has its own data breach notification statute, with varying definitions of personally identifiable information, or PII, and different notification time frames. These statutes generally require entities to notify affected individuals and, in some cases, state regulators or consumer reporting agencies, when a breach involving PII occurs. The specifics of what constitutes PII and the required notification timeline can differ from state to state.

Under HIPAA, covered entities and their business associates are required to implement administrative, physical and technical safeguards to protect electronic PHI. When a breach of unsecured PHI occurs, entities must comply with HIPAA's Breach Notification Rule. This rule may require notifications to individuals, the secretary of the U.S.

Department of Health and Human Services, other affected covered entities, and potentially the media.

Strategies for Resilience

1. Backup Plans

It is uncommon to reference famous boxers when discussing cybersecurity. However, Mike Tyson's well-known quote is particularly relevant to the responses observed following many cybersecurity incidents: "Everyone has a plan until they get punched in the mouth."

Prior to these large-scale cybersecurity incidents, many healthcare entities lacked incident response plans, business continuity plans or disaster recovery plans.

Even when an organization had an incident response plan, they often did not fully anticipate operational impacts resulting from incidents outside their own IT environment, which can affect patient and financial operations, e.g., billing- or claims-related processes.

For example, if a cyberattack on a business associate causes widespread operational disruptions for covered entities relying on the business associate's services, the business associate's incident response plan may not have considered the broad impact. This can leave downstream covered entities struggling to conduct their business.

While it might seem that each covered entity should handle this on their own, the business associate also has a vested interest in maintaining business and partnership relationships.

If you cannot be seen as a trusted partner who can withstand these types of disruptions, you are likely to lose business. Therefore, it's crucial to consider how incidents will affect both your own environment and operations, as well as those who rely on your services.

To address this scenario, both healthcare entities and the business associates they rely on should incorporate established operational workarounds within their incident response plans and business continuity plans.

These plans should consider not just their own systems being down, but also those of their partners. Covered entities that are prepared with an alternate service provider built into their incident response plan, or business associates who have a Plan B in case a system goes down, may be able to quickly pivot rather than be forced to watch their business operations stagnate.

2. Knowing Your Role

It is a necessity for healthcare entities to have a clear understanding of their roles and the data they manage.

HIPAA distinguishes between a covered entity, i.e., a data owner, who receives PHI in the course of carrying out healthcare activities for patients, and business associates, i.e., a service provider, who perform functions or activities for a covered entity that involves the use or disclosure of PHI.

While many organizations expect the entity experiencing the incident to provide notice, a business associate's breach notification obligations under HIPAA only require that it notify an affected covered entity no later than 60 days following the discovery of a breach.[3]

However, contractual notification obligations and business relationship considerations often result in tighter notification timeframes and business associates shouldering some, if not all, of the reporting obligations on behalf of a covered entity.

HHS guidance makes clear that regardless of the nature of the incident, the primary responsibility for notification after a data breach lies with the covered entity. However, business associates certainly take on this responsibility on behalf of covered entities in various circumstances. In fact, the HHS guidance explicitly addresses this scenario:

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual. [4]

For the healthcare industry, recent times have demonstrated that notification following large-scale incidents suffered by business associate service providers is not straightforward.

For example, even though not required under HIPAA, it may be a sound strategy for a business associate to provide notice on behalf of covered entities to ensure consistency of messaging rather than having hundreds of covered entities notifying patients and regulators about the same incident in different ways.

For covered entities, this approach ensures the covered entity complies with their notification obligations under HIPAA, while aligning with the actions of other affected organizations, avoiding unnecessary attention or scrutiny.

Given the complexities surrounding data ownership during large-scale incidents affecting business associates, both covered entities and business associates can benefit from two key preparations: (1) understanding their roles under HIPAA before any incident occurs; and (2) establishing a response plan or protocol for incidents involving business associates, which can be included in an incident response plan or within vendor contracts.

This ensures that notification responsibilities are clearly established, leading to a more seamless and timely notification process.

3. Early Regulatory Involvement

The idea of reporting an active cybersecurity incident to a regulatory body is often unappealing to many organizations. Inviting regulatory scrutiny during the investigation and recovery phases can feel like adding additional burdens at an already stressful time.

If an incident is likely to have a widespread impact on patient services or involve PHI, notifying regulators early in the response process can be beneficial. Early notification opens lines of communication and provides transparency, which regulators may view favorably.

This is especially important for incidents affecting patient care or healthcare operations, as regulators often receive inquiries from concerned citizens. Regulators may find it useful to know the current status of the response, any workarounds that have been implemented, and additional details that can help with their discussions with consumers.

While regulators are not likely to provide legal guidance, they may be willing to collaborate with you on the response and offer suggestions on how to assist potentially affected individuals.

If managed correctly, this collaboration can be seen as regulators working with you to resolve the incident, rather than just reacting to it. Understanding the key regulators who may be involved following an incident and what their expectations are is crucial to leveraging this strategy effectively.

It is important to acknowledge that this is not a one-size-fits-all approach. Some entities may be justified in waiting to notify affected individuals and applicable regulators until they fully understand the scope and impact of an incident.

Early collaboration and partnership with regulators in responding to an incident is just one example of creative approaches to incident response that could better position an organization for any regulatory or litigation issues that follow.

Moving away from the idea that incident response is cookie-cutter and taking the time to think through and anticipate the issues that arise during incident response will lead to more favorable outcomes for everyone involved.

---

[1] 2025 Verizon Data Breach Investigations Report.

[2] https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec.

[3] 45 CFR 164.410(b).

[4] Breach Notification Rule | HHS.gov https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- Privacy + Cyber