5 Steps For Counsel Managing Health Care Data Breaches

By **Gina Bertolini, Jacqueline Hoffman and Desiree Moore** (March 18, 2022)

Gina Bertolini

Jacqueline Hoffman

Desiree Moore

Recent escalations of data security incidents and data breaches have significantly affected companies across many industries. According to the Identity Theft Resource Center, the U.S. experienced a staggering 68% increase in the total number of data compromises in 2021 as compared to 2020.[1]

This threat is felt acutely within the health care sector, given the sensitivity of data and the complex, intersecting regulatory framework governing data privacy and security in the health care setting.

Additionally, innovations in technology have expanded traditional models of health care, resulting in the proliferation of health-care-adjacent entities.

As a result, many new or evolving companies that are not traditional health care providers may find themselves subject to the Health Insurance Portability and Accountability Act, either as covered entities or business associates or subcontractors to business associates, including, for example, information technology developers such as developers of mobile applications, telehealth platform solutions and artificial intelligence programs.[2]

It is critical that any company involved in a data security incident or breach involving health information be mindful of the relevant legal framework and take adequate steps to remedy the situation without delay.

The following scenario illustrates five important steps to managing a data security incident[3] in the health care sector:

The client, an ancillary health care provider, has had a data security incident. Within the first few hours of the incident, the client calls your office for legal advice. The client is unsure of the depth and scope of the incident; however, they believe that it is a ransomware event because their systems are locked, their files are encrypted, and their business operations are significantly interrupted. The client has engaged its information technology resources to mitigate any ongoing risk to data and now has asked for legal assistance.

Step One: Consider the Client's Legal Obligations in the Event of a Breach

In managing a data security incident, it is imperative — and most protective of the company — for legal counsel to quickly partner with the client to assess and prepare a coordinated, strategic response that addresses every aspect of a breach.

Once the client is aware of the incident, the clock has started running on potential notice and reporting obligations. Health care security breaches raise complex and interweaving technical, operational and regulatory challenges, including: ongoing risk to the integrity and security of the data; threats to patient safety caused by corrupt or inaccessible data; management of workforce response; and the likelihood of a government investigation

resulting in increased scrutiny of the client's privacy and security programs more broadly.

Additionally, entities grappling with a security incident may be required to issue expedited — and, depending on how much information is initially available, possibly interim — notices to affected individuals, the media, and state and federal regulators. Concurrently, such entities should be cognizant of avoiding taking actions in response to the threat that exacerbate security risks or result in another breach.

Step Two: Investigate Internally, Collaborate With Third Parties and Gather Internal Documentation

As part of legal counsel's early evaluation and analysis of events, the client's internal IT department should be involved, under the protection of the attorney-client and work-product privileges, to assess actions taken since discovery of the incident, and to confirm termination of the initial intrusion or breach and mitigation of ongoing risks.

Typically, the client's IT department, given its internal role in managing data, is best situated in the initial phases of an incident to identify critical details essential to assessing the incident and determining an appropriate course of action.

In many instances, the client will then require a third-party forensic team to assess the nature and scope of the incident, along with its root cause. Legal counsel should engage these third-party teams to preserve the attorney-client and work-product privileges where possible.

Legal counsel should be prepared to support the client's team in analyzing and determining risks associated with whether — and to what extent — the client will pay a ransom for incidents that involve a ransomware attack; in notifying law enforcement, as appropriate; and in liaising with the client's insurance company.

In doing so, it is important to be aware of whether and what other federal regulations apply and whether paying the ransom could subject the client to enforcement action under those regulations.[4]

During this time, counsel and the client can assess whether an internal or external facing statement is appropriate, depending on the severity of the incident and the impact to employee operations and patient or consumer trust and well-being, and determine who should be informed of the incident on an informal basis while client and counsel further investigate.

Also during this time, legal counsel can assist the client in gathering its internal and external policies and procedures related to the access, use and disclosure of protected health information and other individually identifiable health information, as appropriate.

Step Three: Conduct a HIPAA Risk Assessment

Working together, legal counsel, third-party investigators and the client will need to determine the nature of the data affected by the incident and the extent of impact.

As further outlined below, the client will need to determine whether the incident compromised the security or privacy of the protected health information, in which case it is a breach under HIPAA's breach notification rule,[5] or otherwise resulted in an unauthorized disclosure of individually identifiable health information, which may require an analysis

under other relevant laws.

For covered entities and business associates, this analysis will include an initial assessment of whether any of the data at issue is protected health information that is covered by HIPAA's privacy and security rules.[6]

HIPAA broadly defines protected health information as individually identifiable information that is created or received by a health care provider or health plan; is transmitted, sorted or maintained in electronic media; and relates to the past, present or future physical or mental health or condition of the individual.

Protected health information includes demographic information, including names, dates, addresses, states and zip codes. Generally, any individually identifiable information captured as part of a health care transaction or service is protected health information.

An acquisition, access, use or disclosure of protected health information in a manner not permitted under HIPAA's privacy rule is presumed to be a breach, unless the company can demonstrate that there is a low probability that the protected health information has been compromised based on a risk assessment that considers at least the factors outlined in the breach notification rule.

Accordingly, once legal counsel determines that the data at issue is protected under HIPAA, counsel will analyze the facts and circumstances of the cybersecurity incident carefully and objectively to assess the nature and extent of the protected health information involved, the unauthorized person who used the protected health information or to whom such disclosure was made, and other factors outlined in HIPAA's breach notification rule.

The analysis must consider whether and to what extent the impermissible acquisition, access, use or disclosure of protected health information compromised the security or privacy of the protected health information to determine whether the incident constitutes a breach.

Legal counsel experienced with health care operations and with HIPAA risk assessments and the Office for Civil Rights, which enforces HIPAA, should be able to draw upon other risk assessments and fact patterns to help navigate this analysis.

During this process, counsel also will need to assess if other laws apply to the data affected by the incident. For example, in addition to protected health information, where the individually identifiable health information of individuals is affected, like social security numbers or bank account information, state privacy and security laws may be affected.

Moreover, even if HIPAA is not applicable because the parties involved are not covered entities or business associates, and patients or consumers authorized the disclosure of protected health information to the client, if the data at issue is health information, clients should be aware that the Federal Trade Commission's health breach notification rule[7] might be applicable.

Counsel can work with the client to map out how the various applicable laws define the data and carefully determine which reporting requirements under each law are applicable.[8]

It is important for both the client and counsel to keep in mind that the steps outlined in this article may need to take place concurrently. For example, this discussion is not mutually exclusive from preparation of reporting and notices; the regulatory requirements and

timelines described in step four may precede the completion of a robust investigation and risk analysis.

At that point, the client along with counsel must, without delay, be aware of its obligations to timely comply with regulatory reporting and the knowledge that amending an agency report and even perhaps secondary notices may be required.

Step Four: Provide Notice and Begin an Internal Evaluation

In the event of a breach under HIPAA's breach notification rule, or a breach that otherwise implicates the FTC health breach notification rule or state data privacy laws, the client will need to take immediate steps to mitigate the breach and notice the affected individuals.

If more than 500 individuals are affected, the company will need to report the incident to OCR and notify the media as soon as reasonably possible, but no later than 60 days from discovery of the breach.[9]

Typically, legal counsel will work with the client to provide notices to OCR, relevant state attorneys general and affected individuals, the latter of which requires a brief description of the incident, including date of the breach and date of discovery, a description of the types of unsecured protected health information involved in the breach, and steps individuals should take to protect themselves.

Counsel also can assist in preparing notices to media, if required, and talking points and FAQs for the company to use, for example, as part of a toll-free call center that may be required to answer questions related to the incident.

Further, counsel will coordinate with the company if and when a state attorney general and/or OCR initiates an inquiry or investigation, to help the client navigate the nuances involved in that process. As these initial steps unfold, the client should continue efforts to mitigate the impact of the incident, restore the various affected systems and return to its ordinary course of business.

In addition to providing notice to any required parties, the client should conduct an assessment of its IT and security policies, procedures, workforce education practices and security systems in light of the breach, and make any necessary revisions in accordance with guidance from counsel and any third-party data security auditors that the client may retain.

Doing so is important both from the standpoint of ensuring adherence to best practices for data protection, and for demonstrating to regulators that the client views data breaches as a serious threat and is making a good faith effort to prevent future data loss.

Step Five: Respond to Regulatory Inquiries

In the aftermath of a data breach in the health care space, it is likely that a client will receive a follow-up inquiry — if not a more fulsome and formal investigation — from OCR and possibly state attorneys general.[10]

Both of these processes can be lengthy, involving significant internal work to collect documents and information, update policies and procedures, and engage in numerous exchanges with government regulators, typically OCR.

While the information gathering and preparation of responses to several regulatory bodies may seem redundant, the client's responses will need to be sufficient to independently address the discrete requirements of each regulatory body involved.

Conclusion

In the current cybersecurity space, the question of data security incidents is not "if," but "when," they will happen. Although the early stages of dealing with a data security incident can be daunting, the five-step road map above condenses the initial important steps into tangible action items that will help counsel and companies work together to mitigate harm to patients and consumers, protect critical data, improve systems and operations, and effectively navigate government investigations.

Gina Bertolini is a partner at K&L Gates LLP.

Jacqueline Hoffman is a partner at the firm.

Desiree Moore is a partner, and founding member and co-lead of the digital crisis planning and response client solution, at the firm.

K&L Gates associates Kenneth Kennedy and Kelsi Robinson contributed to this article.

[1] Identity Theft Resource Center, "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises" (January 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/).

[2] Even where health-adjacent organizations are not subject to HIPAA, FTC's Health Breach Notification Rule, as well as State confidentiality and data protection laws may apply.

[3] HIPAA's Security Rule defines "security incident" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system" (45 CFR 164.304), and a "breach" is the "acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted" under HIPAA's Privacy Rule that compromises the security or privacy of the PHI (45 CFR 164.402(1)). Thus, not every security incident will result in a breach under HIPAA. Under FTC's Health Breach Notification Rule, "breach" is more broadly defined to include the unauthorized acquisition of certain individually identifiable health information (IIHI) (16 CFR 318.2). We use the term "incident" in this article to address interference with system operations and the unauthorized access, use, disclosure, modification, or destruction of PHI or IIHI, the latter of which is not necessarily considered PHI due to the data and the actors involved, and we reiterate that a key component in the management of any security incident is assessing whether it resulted in a "breach" under HIPAA's Breach Notification Rule and the FTC's Health Breach Notification Rule.

[4] Counsel should be aware of and will assist the client in understanding the importance

and application of federal regulatory guidance relating to how to respond to a ransomware attack, including whether and when to pay the ransom in a ransomware attack and whether paying a ransom could expose the client to sanctions. See, e.g., FBI, "Ransomware" (available at https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware); FTC, "Ransomware Prevention: An Update for Businesses," (available at https://www.ftc.gov/news-events/blogs/business-blog/2020/12/ransomware-prevention-update-businesses); Department of the Treasury, Office of Foreign Assets Control (OFAC), "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payment," available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf. This article will not go into detail about OFAC guidelines and potential sanctions for running afoul of such guidelines, but it is imperative to be mindful of them and work closely with legal counsel to understand the implications to any specific breach scenario.

[5] 45 CFR 164.400 through 164.414.

[6] We note that business associates are directly subject to certain security and confidentiality compliance requirements under HIPAA and HITECH, and may be directly subject to penalties for noncompliance. See 78 Fed. Reg. 5,566, 5,591-2 (January 25, 2013); 45 CFR 164.502(a)(3)-(4), (b), (e)(1)(ii).

[7] 16 CFR Part 318.

[8] Relevant state laws will include any state in which an individual whose IIHI was affected by the incident resides. To the extent the company is global, additional jurisdictional considerations will apply.

[9] In parallel, clients may need to notify state Attorneys General or other regulatory agencies that may apply and may, sooner than HIPAA, require such notice and disclosure.

[10] While anecdotal, heightened enforcement activity individually undertaken by certain states or collectively with the combined efforts of several states' attorneys general suggest that state actions and resolutions need not wait for OCR. Recent state actions, such as the announcement by New York Attorney General Letitia James of a $600,000 settlement with vision benefits provider EyeMed resulting from a healthcare data breach that compromised PHI of over 2 million people, is illustrative of a rise in breaches as the result of cyber-attacks, as well as heightened government enforcement, specifically state enforcement actions.