

Breach Preparation: Building a Legally Defensible Cybersecurity Breach Response

by **Rebecca Rakoski** | *XPAN Law Partners, LLC*

Cybersecurity incidents are no longer theoretical risks. This is especially true for health care entities, health plans and benefit plans regulated by the Employee Retirement Income Security Act (ERISA). Cybersecurity incidents are operational inevitabilities in a threat environment where protected health information (PHI), personally identifiable information (PII) and plan-related financial data are among the most valuable assets targeted by threat actors.

For organizations subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Department of Labor (DOL) Cybersecurity Program Best Practices, the consequences of a breach extend beyond operational disruption.[1] A breach implicates regulatory compliance, fiduciary duty, litigation exposure and governance oversight.

Preparation and response must therefore be structured not merely as technical exercises but as legally informed risk management functions.

AT A GLANCE

- Cybersecurity is a legal and fiduciary obligation for entities covered by the Health Insurance Portability and Accountability Act (HIPAA) as well as Employee Retirement Income Security Act (ERISA) plans.
- Essential elements of a legally defensible cybersecurity breach response plan include a documented risk analysis, tested incident response plan and strong third-party/vendor oversight.
- Engaging legal counsel early may help benefit plans preserve attorney-client privilege, meet notification duties and create documentation that may help them avoid regulatory issues and litigation.

The Regulatory and Fiduciary Framework for Breach Preparation

HIPAA-covered entities and business associates operate under the HIPAA Security Rule, which requires them to conduct an accurate and thorough risk analysis and to implement administrative, physical and technical safeguards to protect electronic PHI.[2] In addition, the HIPAA Breach Notification Rule imposes strict timing and content requirements when unsecured PHI is compromised.[3] A failure to comply can lead to significant civil monetary penalties and multiyear corrective action plans imposed by the Office for Civil Rights (OCR).

Plan sponsors and fiduciaries of ERISA plans, such as retirement plans, face parallel but distinct obligations. The DOL has made clear that cybersecurity is a matter of fiduciary prudence. Plan fiduciaries must act with care, skill, prudence and diligence in protecting participant data and plan

assets. The DOL's cybersecurity guidance emphasizes prudent selection and monitoring of service providers, implementation of strong security controls and the development of documented incident response procedures. Inadequate cybersecurity practices can form the basis of fiduciary breach claims, particularly where participant accounts or plan assets are compromised.

In both contexts, regulators and courts evaluate not only whether a breach occurred, but whether leadership acted reasonably before and after the event.

Building a Legally Defensible Cybersecurity Program

Essential elements of a cybersecurity program include the following.

Risk Analysis

Preparation begins with a comprehensive and regularly updated risk analysis. HIPAA requires this risk analysis to be documented. Documenting the risk analysis also supports fiduciary prudence under ERISA. The risk analysis should be aligned with regulatory expectations and cover remediation priorities.

When structured properly, portions of cybersecurity assessments and forensic analyses may also be conducted under attorney-client privilege, providing strategic protection in the event of future litigation or regulatory scrutiny.

Incident Response Plan

An incident response plan is as essential as the risk analysis. But a document sitting on a shelf collecting dust is not sufficient. The plan must clearly define what constitutes a security incident versus a reportable breach, establish escalation protocols and designate decision makers.

Vendor Oversight

Vendor oversight is another important area since many cybersecurity breaches originate with third-party service providers. HIPAA requires compliant business associate agreements, and DOL guidance requires fiduciaries to prudently select and monitor service providers. Plans should review vendor contracts for cybersecurity representations, indemnification provisions, insurance requirements, audit rights and breach notification time lines. Contractual gaps discovered after a breach frequently expose organizations to what is later understood to be avoidable financial and legal risk.

Other Elements

Plans should also evaluate workforce training, access controls, encryption standards and cybersecurity insurance with HIPAA and DOL compliance guidelines in mind. Policies should be technically sound and also aligned with enforcement trends and defensible in a regulatory investigation.

Putting Preparedness Policies Into Practice

Even well-drafted policies fail without operational discipline. Regulators and courts increasingly expect organizations to demonstrate not only that controls exist, but that they are tested, understood and consistently followed in practice. Preparedness therefore requires a continuous, organization-wide effort that integrates legal, technical and business functions.

Preparedness is an ongoing process that needs to reflect the evolving threat landscape, regulatory expectations and organizational complexity. Entities that treat cybersecurity planning as a one-time compliance exercise often find themselves unprepared when a real-world incident unfolds under time pressure and uncertainty.

Key components of operational preparedness include the following.

Tabletop Exercises and Simulations

Incident response plans should be tested through regular tabletop exercises involving executive leadership, IT, compliance, communications and legal counsel. These exercises should simulate realistic scenarios, including ransomware attacks, vendor compromises and unauthorized access to sensitive data. In addition to assessing the technical response, the objective is to test that response and also evaluate decision making, escalation timing and coordination across functions. Documentation of these exercises can later serve as evidence of reasonable preparation.

The Role of Counsel in Cybersecurity Preparedness and Response

The plan attorney is a central participant in shaping a legally defensible posture before, during and after a breach.

Before

In the preincident phase, counsel can help guide risk analyses to ensure alignment with Health Insurance Portability and Accountability Act (HIPAA) requirements and fiduciary standards, structuring vendor agreements to address cybersecurity obligations and liability exposure, and integrating legal considerations into incident response planning, including strategies for preserving privilege. Counsel also advises on documentation practices that will later be scrutinized by regulators and courts.



During

During an incident, counsel often directs the engagement of forensic investigators in a manner designed to preserve attorney-client privilege where appropriate, while also interpreting key legal standards such as HIPAA's "low probability of compromise" analysis. In more complex scenarios, including ransomware events, counsel provides guidance on regulatory expectations, potential Office of Foreign Assets Control (OFAC) implications and coordination with law enforcement. Just as importantly, legal counsel helps oversee communications to regulators, affected individuals and other stakeholders to reduce the risk of inconsistent or premature disclosures.

After

Following an incident, counsel can manage regulatory inquiries and enforcement actions, support litigation strategy, and guide remediation efforts and governance reporting. Perhaps most importantly, counsel helps establish and preserve a documented record of reasonable and informed decision making, which is often central to defending the organization's actions in both regulatory and litigation contexts. Organizations that integrate legal counsel into cybersecurity planning and response frameworks from the outset should be better positioned to demonstrate prudence, diligence and compliance.

Clearly Defined Roles and Escalation Authority

During an incident, uncertainty about who is responsible for decision making can significantly delay response efforts. Organizations should establish clear lines of authority for incident declaration, regulatory notification decisions, engagement of third-party vendors and public communications.

Identification of External Resources

Plans should identify in advance forensic investigators, breach response counsel, notification vendors and public relations firms. Where appropriate, these relationships should be structured so that vendors can be engaged through an attorney, which may allow certain investigative activities to be conducted under privilege. Delays in identifying qualified vendors during an incident often lead to increased exposure and missed regulatory deadlines.

Data Mapping and Information Governance

Organizations must understand where sensitive data resides, including PHI, PII and plan-related financial data. Without accurate data mapping, it becomes significantly more difficult to assess the scope of an incident, determine notification obligations and respond within required time frames.

Documentation and Audit Readiness

Preparedness is ultimately measured through documentation. Risk analyses, training records, vendor due diligence and incident response testing should be maintained in a manner that demonstrates continuity, consistency and leadership oversight. Regulators routinely request this information following an incident.

Alignment With Cybersecurity Insurance Requirements

Cybersecurity insurance policies frequently include specific requirements related to incident reporting, vendor engagement and cooperation during investigations. Preparedness efforts should be aligned with these obligations to avoid jeopardizing coverage at the time it is most needed.

Organizations that implement preparedness in this manner are better positioned not only to respond effectively to an incident, but also to demonstrate that their actions before and after the event were reasonable, deliberate and aligned with regulatory expectations.

The Critical First Hours After a Breach

The first 72 hours following the discovery of a potential breach often determine the organization's long-term exposure. Once a cybersecurity incident is suspected, previously identified counsel should be notified immediately so that forensic experts can be retained through counsel where appropriate. This structure may also allow investigative findings to fall within the protection of attorney-client privilege or work-product doctrine, depending on jurisdiction and circumstances.

Key determinations following the breach include whether PHI or plan data has been accessed, acquired or exfiltrated. Under HIPAA, there is a presumption of breach unless the organization or entity can demonstrate a low probability that PHI has been compromised based on a documented risk assessment considering specific regulatory factors. Such analysis is highly fact-specific and legally nuanced. Inadequate documentation or misapplication of the standard can significantly increase enforcement risk.

Regulators generally treat ransomware incidents as presumed breaches. Plans must assess regulatory guidance, potential Office of Foreign Assets Control (OFAC) implications, contractual obligations and coordination with law enforcement. Decisions regarding ransom payments carry a host of implications, including legal, financial and reputational.

Notification Obligations and Communication Strategy

If breach notification is required under HIPAA, affected individuals must be notified without unreasonable delay and no later than 60 days following discovery. The content of these notifications is regulated, and inaccuracies can compound liability. In large-scale breaches, notification to the Department of Health and Human Services (and, in certain cases, media outlets) is also required.

For ERISA plan fiduciaries, while there is no direct analogue to the HIPAA Breach Notification Rule, fiduciaries must consider their obligations under plan documents, fiduciary duties of prudence and loyalty, and potential participant communications. Participant lawsuits increasingly allege that fiduciaries failed to implement reasonable cybersecurity measures. The documentation of deliberative processes and legal consultation can be essential in defending such claims during both prelitigation and trial.

Plans also should follow a public relations strategy. For example, statements made prematurely or without full forensic understanding may later be heavily scrutinized by regulators or plaintiffs' counsel. Coordinated legal and communications planning reduces the risk of inconsistent or misleading disclosures.

Postincident Scrutiny and Governance Oversight

Regulatory review often focuses as much on postincident remediation as on the breach itself. OCR investigations routinely request documentation of prior risk analyses, policies, training materials and board oversight. The DOL similarly evaluates whether fiduciaries exercised appropriate oversight of service providers and cybersecurity programs.

Boards of directors and fiduciary committees should be formally briefed on significant cybersecurity incidents, remediation measures and program enhancements. Governance documentation should reflect active oversight and informed decision making.

Failure to document corrective action, policy revisions and enhanced safeguards can undermine an otherwise reasonable response. Conversely, thorough documentation can significantly mitigate enforcement penalties and litigation risk.

Cybersecurity as a Legal and Fiduciary Discipline

The prevailing misconception is that cybersecurity is primarily a technical function. For entities subject to HIPAA and DOL cybersecurity guidance, it is equally—

and in some cases, more so—a legal and fiduciary discipline. Regulators and courts assess whether organizations acted reasonably in light of known risks, industry standards and regulatory guidance. This is unequivocally a legal function and behind the reach of tech's expertise. To put a fine point on it, legal counsel provides the interpretive framework necessary to translate technical events into defensible compliance decisions.

In addition, organizations that involve counsel only after regulatory inquiries begin often find themselves at a significant disadvantage from the start, essentially reacting rather than strategically responding at a critical moment when legal strategies/positioning need to be set for the long, winding road of litigation. By contrast, it cannot be made clear enough that integrating legal guidance into cybersecurity planning, incident response design, vendor contracting and governance oversight creates a defensible record of prudence.

In today's enforcement climate, the question is not whether a breach will occur, but whether leadership can demonstrate that it prepared responsibly and responded appropriately when a breach does occur. Similar to preparing for a rainy day, the early and continuous involvement of experienced legal counsel for HIPAA-covered entities and ERISA fiduciaries alike is not simply advisable—It is a necessary and inevitable component of regulatory compliance and fiduciary duty. BQ

AUTHOR



Rebecca Rakoski is the co-founder and managing partner at XPAN Law Partners LLC, a boutique cybersecurity and data privacy law firm located in the Philadelphia, Pennsylvania region. She reviews and analyzes her clients' legal obligations and works to create tailored cybersecurity and data privacy programs. As a recognized thought leader in data privacy and cybersecurity law, she serves on the New Jersey State Bar Association's Cyber Task Force. She can be reached at rrakoski@xpanlawpartners.com.

Endnotes

1. "DOL Cybersecurity Program Best Practices," www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.
2. Health Insurance Portability and Accountability Act (HIPAA) Security Rule, www.hhs.gov/hipaa/for-professionals/security/index.html.
3. HIPAA Privacy Rule, www.hhs.gov/hipaa/for-professionals/privacy/index.html.

International Society of Certified Employee Benefit Specialists

Reprinted from the Third Quarter 2026 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.

©2026 International Society of Certified Employee Benefit Specialists

pdf/826