

IT-659 Cybersecurity Policy Development

Cyberlaw & Ethics — Incident Report & Legal Analysis

Logan Garth Goodwin
Southern New Hampshire University
August 2025

This document demonstrates application of cybersecurity principles, legal compliance analysis, ethical evaluation, and regulatory standards within a real-world healthcare data breach case.

Logan Goodwin

Michael Adams, Adjunct Instructor (MSc, CCISO, CISM, CISSP)

IT-659 Cyberlaw & Ethics

08/04/2025

9-2 Final Project Submission Information Technology Incident Report and Summary

Application of Cyberprinciples

To protect patient information and uphold trust in the healthcare sector, it's crucial to implement fundamental cybersecurity principles: confidentiality, integrity, availability, and accountability. Maintaining confidentiality ensures that only authorized individuals can access sensitive data, such as patients' Social Security numbers, diagnoses, and treatment records. This principle is in direct agreement with the HIPAA Security Rule, which mandates administrative, technical, and physical protections for protected health information (U.S. Department of Health & Human Services, 2024).

Maintaining accurate and unaltered patient data through integrity is vital for clinical decisions, billing procedures, and, most importantly, patient safety. Tampering with medical records, to illustrate, can cause patients to receive incorrect medical care or medication. Availability means healthcare providers and patients can access data whenever they need it, which helps them provide and receive timely, effective care. Interruptions in treatment plans and compromised patient outcomes can result from downtime or data loss.

It is the responsibility of healthcare organizations to manage risk, put controls in place, and respond to incidents. Maintaining audit trails, performing regular risk assessments, and guaranteeing staff adherence to security policies and procedures are all part of this principle. Adopting these cyberprinciples allows healthcare organizations such as Trinity Health to comply with legal mandates, strengthen ethical conduct, minimize operational hazards, and safeguard public faith in digital healthcare (Federal Trade Commission, 2016). These principles are vital in the current era of e-commerce and e-communication. They create a base for securing data in complex networks, defending against new threats, and complying with changing laws.

Summary of Case

A data breach occurred at Trinity Health, the incident in question, which is a healthcare system based in Livonia, Michigan, operating Mercy Health Network and Mercy Medical Center Clinton in Iowa. In the period spanning March 7 and April 7, 2023, email systems holding the personal and medical details of about 21,000 patients were compromised by unauthorized individuals (Alder, 2023). Patient names, addresses, birth dates, Social Security numbers, diagnosis codes, treatment details, prescription data, and discharge information were among the highly sensitive data included in the breach.

Trinity Health identified the data breach on April 4, 2023, almost a month after the initial intrusion. Once the organization detected the issue, it secured its systems and gave affected patients twelve months of complimentary credit monitoring. Although these efforts were made, a class action lawsuit was brought against Trinity Health, Mercy Health Network, and Mercy Medical Center Clinton on June 12, 2023. The lawsuit alleges violations of the HIPAA Security Rule, negligence, breach of contract, and inadequate monitoring that allowed attackers to remain undetected for an extended period (U.S. Department of Health & Human Services, 2024).

The incident attracted public attention because it demonstrated systemic gaps in intrusion detection, breach response, and communication with affected patients. Trinity Health faced significant reputational damage and legal consequences, and the breach underscored the critical need for stronger cybersecurity measures within the healthcare sector. Although the attackers have not been uncovered, the lawsuit emphasized the organization's responsibility to protect patient data and highlighted deficiencies in its security posture that ultimately compromised patient trust (Federal Trade Commission, 2016).

Ethical Issues

The data breach at Trinity Health reveals significant ethical shortcomings related to patient privacy, transparency, and organizational responsibility. At its core, the breach reflects a failure to uphold the ethical duty to proactively protect sensitive patient information from foreseeable risks. Healthcare organizations hold a unique ethical obligation to protect patients' private health data, not only because it is legally mandated but because it directly affects individuals' dignity, trust, and well-being. By failing to detect and contain the breach for nearly a month, Trinity Health exposed patients to an extended period of vulnerability, increasing the risk of identity theft and other forms of harm.

Equally concerning is the organization's approach to communication after the breach. The class action lawsuit against Trinity Health alleged that the notifications sent to patients were insufficient and failed to provide meaningful information about what had happened, what data was compromised, and what steps were being taken to mitigate further risk (Alder, 2023). From an ethical perspective, this lack of transparency undermines the trust patients place in healthcare providers and fails to respect patients' right to make informed choices about protecting themselves after an incident.

The organization's apparent lack of proactive monitoring and timely risk assessments suggests an ethical lapse in balancing operational efficiency against patient safety. While no organization can guarantee perfect security, ethical practice requires continuous investment in detection systems, staff training, and robust response plans to reduce the likelihood and impact of breaches. In Trinity Health's case, these shortcomings contributed to the scale and duration of the incident, highlighting a gap between compliance obligations and the broader ethical responsibility to safeguard those who rely on the organization's services (U.S. Department of Health & Human Services, 2024).

Legal Compliance

Trinity Health was legally required to adhere to the HIPAA Security Rule at the time of the event; this rule outlines the necessary administrative, physical, and technical controls for securing protected health information (U.S. Department of Health & Human Services, 2024). A key element of this framework involves risk assessment, ongoing monitoring, and the ability to detect and respond to incidents. Attackers maintaining access to Trinity Health's systems for close to a month reveals deficits in these

areas. Because of this long-lasting unauthorized access, patient information was more likely to be compromised, and the organization failed to meet its legal obligation to be prompt with preventing, noticing, and reacting to security breaches.

The class action lawsuit, filed in June 2023, also pointed to alleged violations extending beyond HIPAA. The lawsuit alleged Trinity Health did not adhere to industry best practices for safeguarding sensitive information, citing Federal Trade Commission guidelines that mandate reasonable security measures relative to the sensitivity of the data (Federal Trade Commission, 2016). The failure of Trinity Health to adequately monitor its systems, implement multi-factor authentication on specific platforms, and promptly identify the breach created an environment where attackers could exploit vulnerabilities, causing considerable legal ramifications.

The response of Trinity Health to the data breach has drawn criticism due to the lack of adequate support and detailed notifications to the patients affected. HIPAA's Breach Notification Rule mandates that covered entities promptly inform affected individuals of a breach with specific details, but the lawsuit asserts that Trinity Health's communication was insufficiently transparent and lacked reassurance. Taken as a whole, these legal compliance deficiencies illustrate that inadequate policy execution and monitoring may trigger regulatory sanctions, as well as enduring harm to an organization's image and bottom line.

Societal and Cultural Impact

The data breach at Trinity Health had broader societal and cultural affects that extend beyond immediate legal consequences. In healthcare, patient trust is foundational; when sensitive data such as Social Security numbers, medical diagnoses, and treatment details are compromised, it undermines confidence in digital health systems and electronic medical records. For patients, especially those in vulnerable or underserved communities served by Mercy Health Network and Mercy Medical Center Clinton, the breach heightened fears of identity theft and potential misuse of personal information. This erosion of trust can discourage patients from fully disclosing health details or from using digital tools like online portals and telehealth platforms, which are increasingly critical for modern care delivery.

Culturally, the incident reinforces growing public skepticism about how large organizations handle personal data, especially in sectors like healthcare where the stakes are high. It also highlights concerns about the ethical responsibility of institutions to go beyond minimal compliance and adopt proactive measures that truly protect individuals. The breach demonstrates that failures in cybersecurity are not purely technical or legal issues but also social issues that affect real people's willingness to engage with healthcare providers, share truthful information, and rely on digital systems. In the longer term, repeated breaches across the industry risk creating a culture of fear and avoidance that could undermine efforts to improve patient outcomes through technology and data-driven care.

Regulations

While the Trinity Health breach didn't immediately trigger new federal legislation, it highlights the role such incidents play in the wider regulatory discussions surrounding data security and patient privacy. The rise of comparable healthcare breaches has led regulators to reinforce the HIPAA Security Rule with an emphasis on real-time monitoring, timely breach detection, and comprehensive risk assessments (U.S. Department of Health & Human Services, 2024). Across the healthcare industry,

state governments have responded to recurring incidents by implementing more stringent breach notification laws, faster reporting requirements, and higher financial penalties for those who do not comply.

This breach corresponds to larger regulatory shifts spurred by well-known incidents in different industries. The Federal Trade Commission, for instance, has maintained that deficient data protection procedures may represent unjust or misleading actions as defined by Section 5 of the FTC Act (Federal Trade Commission, 2016). Even though the FTC's direct authority over healthcare data is limited by HIPAA, this guidance reinforces the idea that organizations must proactively handle cybersecurity risks rather than reactively respond.

The push for overarching federal data privacy legislation covering personal data receives support from cases such as Trinity Health. Organizations are increasingly expected by regulators to go beyond minimum compliance and embrace industry standards and frameworks like NIST SP 800-53 or HITRUST CSF to prove they have reasonable security measures. Therefore, although the Trinity Health breach did not alter any laws, it highlights the increasing regulatory pressure on organizations to be more responsible for preventing, detecting, and responding to data breaches.

Standards

Following the Trinity Health data breach, it became clear that the organization's security measures failed to align with both industry benchmarks and broader IT standards for adequate cybersecurity. Within healthcare, the HIPAA Security Rule establishes required administrative, physical, and technical safeguards to protect patient data (U.S. Department of Health & Human Services, 2024). Trinity Health's failure to detect unauthorized access for nearly a month suggests weaknesses in continuous monitoring and incident response planning, which are fundamental elements of these safeguards.

Beyond HIPAA, organizations are encouraged to align with widely recognized frameworks such as NIST SP 800-53, which outlines detailed security and privacy controls, and the HITRUST CSF, which integrates multiple standards into a single certifiable framework tailored for healthcare. Similarly, the ISO/IEC 27001 standard provides a systematic approach to managing information security risks through documented processes and regular audits. Adoption of these frameworks demonstrates a proactive commitment to data protection that goes beyond minimal compliance.

In Trinity Health's case, alignment with these standards could have strengthened risk assessments, required multi-factor authentication, and mandated more rigorous monitoring systems controls that might have reduced the duration and scope of the breach. The gap between the organization's actual practices and these standards underscores the role of frameworks not only as technical guidance but also as evidence of due diligence when defending against legal and reputational consequences following a breach.

Cultural Impact

Cultural attitudes toward digital healthcare and the broader use of technology for managing personal information were also shaped by the Trinity Health data breach. More and more, patients trust organizations to protect their private information as they use electronic health records, telehealth, and

online portals. Such a large breach undermines trust, leading to worries and disbelief about how safe it is to share personal health details online. Patients, especially those with a history of identity theft or who are from underserved communities, might be unwilling to fully disclose their health information or use digital tools necessary for modern healthcare because of the breach.

This event, besides its impact on individuals, adds to the increasing public sentiment that major healthcare institutions are underfunding cybersecurity efforts, even though they manage extremely sensitive data. Global dissemination of these concerns can occur rapidly through media and social media, magnifying distrust, including among patients who were not directly impacted. The erosion of trust, if left unchecked, could compromise advancements in patient care that rely on data analysis, electronic communication, and the incorporation of innovative technologies such as artificial intelligence. The Trinity Health data breach demonstrates that cybersecurity lapses can trigger extensive cultural effects beyond the direct regulatory and monetary implications, affecting society's attitudes toward and application of information technology in healthcare.

Organizational Changes

We can implement organizational changes that are both practical and effective to better prevent incidents similar to the Trinity Health breach. Initially, Trinity Health may want to consider using an advanced intrusion detection and prevention system leveraging artificial intelligence and machine learning to recognize abnormal patterns and uncover threats that are not limited to known attack signatures. Such technology would significantly reduce dwell time by alerting security teams to suspicious activity earlier. Second, the organization should establish and regularly test a comprehensive incident response plan that clearly defines roles, communication protocols, and objectives, including specific Recovery Time Objectives and Recovery Point Objectives. This would ensure a structured and faster response to future incidents, minimizing potential damage.

Trinity Health should introduce multi-factor authentication for all administrative and privileged accounts to reduce the likelihood of unauthorized access through stolen credentials. Regular role-based security awareness training tailored to different employee groups such as clinical staff, IT teams, and administrative personnel would also improve the organization's human defense layer by addressing specific risks each group faces. These organizational changes would not only enhance detection and response but also reinforce a proactive security culture across all levels of the organization, ultimately reducing the likelihood and impact of future breaches.

Ethical Guidelines

Beyond legal compliance, Trinity Health could adopt stronger ethical guidelines to help prevent future incidents and rebuild patient trust. First, the organization could commit to transparency that goes beyond legal requirements, such as notifying patients promptly of any data exposure, even when the law does not strictly require disclosure. This proactive approach shows respect for patients' right to know and helps them make timely decisions to protect themselves. Second, Trinity Health could establish an internal ethics committee dedicated to reviewing data privacy policies, advising on new technologies, and evaluating data-sharing agreements to ensure ethical considerations remain central to strategic decisions.

These guidelines would encourage the organization to see data protection not merely as a compliance obligation but as a moral duty to protect the individuals whose data they handle. By building policies that prioritize patient autonomy, informed consent, and fairness, Trinity Health can strengthen its reputation and demonstrate a commitment to doing what is ethically right, not just what is legally required. Over time, these measures can foster a culture where protecting patient data is embedded into everyday decision-making and long-term planning.

External Standards

To further reduce the likelihood of future breaches, Trinity Health could adopt and align with recognized external cybersecurity and privacy standards that go beyond basic compliance. Achieving ISO/IEC 27001 certification would demonstrate that the organization has a documented, systematic approach to managing information security risks, verified through external audits. Similarly, integrating the NIST SP 800-53 framework into Trinity Health's security program would provide a comprehensive set of controls covering access management, auditing, and incident response, which are particularly relevant in healthcare. Additionally, adopting the HITRUST CSF could help the organization demonstrate alignment with multiple regulatory requirements, including HIPAA, while offering an industry-recognized benchmark for security and privacy.

These external standards not only strengthen technical defenses but also reinforce accountability and transparency. By implementing them, Trinity Health could show regulators, patients, and business partners that it takes proactive and measurable steps to protect sensitive data. Beyond compliance, these frameworks help organizations identify process gaps, reduce operational risks, and ultimately lower the long-term costs associated with data breaches and regulatory investigations. In today's environment, where trust and reputation are critical, voluntarily aligning with these standards can signal a genuine commitment to data security and patient safety.

International Compliance

Trinity Health's international operations or services to patients from outside the U.S. would necessitate compliance with global data protection regulations, such as the European Union's General Data Protection Regulation. This breach is particularly affected by several articles within the GDPR. Organizations are required by Article 32 to have the right technical and organizational steps to ensure the security of personal data. This involves assessing potential risks and recognizing when incidents occur. Because of Article 33, data controllers must report personal data breaches to supervisory authorities within 72 hours of learning about them, pointing to the significance of fast detection and response. Moreover, Article 35 necessitates organizations to undertake Data Protection Impact Assessments for data processing activities that present a high risk to individuals; these assessments could have identified weaknesses before the breach occurred.

Beyond GDPR, Trinity Health could look to standards like ISO/IEC 27701, which extends ISO/IEC 27001 to create a Privacy Information Management System. This framework helps organizations formalize privacy governance and document how data protection measures meet regulatory obligations. Even for a U.S.-based healthcare provider, adopting these international compliance standards demonstrates an understanding of evolving global expectations and reduces risks associated with cross-border data transfers, partnerships, and services provided to international patients.

Global Cultural Impacts

The Trinity Health data breach, similar to other healthcare breaches, is part of a larger cultural shift impacting global patient confidence in the security and dependability of digital health systems. As these incidents are reported in traditional media and, in particular, across social media platforms, worries regarding data privacy escalate from the local level to encompass a global audience. Fear of compromised data may make patients more hesitant to use online portals, share confidential medical information, or use telehealth services. For example, individuals might choose to withhold family medical history or mental health information, which could ultimately impact the quality of care they receive.

In addition, repeated breaches across the industry risk normalizing the idea that data leaks are inevitable, leading to resignation and reduced trust in healthcare institutions as a whole. This shift can undermine public health initiatives that rely on digital engagement and data collection. On a global scale, these cultural attitudes also create challenges for health systems and technology providers aiming to promote innovations such as electronic health records, artificial intelligence in diagnostics, and data-driven research. The Trinity Health breach thus reflects not only a failure of technical security but also a setback for broader cultural acceptance of digital transformation in healthcare.

Legal and Regulatory Impact

The Trinity Health data breach, together with similar incidents in the healthcare industry, has contributed to growing pressure for stronger and more unified data protection laws both in the United States and globally. While the breach itself did not directly lead to new federal legislation, it adds to the argument for comprehensive national privacy laws that extend beyond HIPAA to cover all forms of personal data. Globally, high-profile breaches have accelerated the adoption of regulations like the European Union's General Data Protection Regulation and influenced laws in countries such as Brazil's Lei Geral de Proteção de Dados and California's California Consumer Privacy Act. These frameworks emphasize principles like accountability, transparency, and prompt breach notification.

In addition, incidents like Trinity Health's highlight the challenges of enforcing consistent data protection standards across jurisdictions, where legal requirements, cultural expectations, and enforcement resources can vary significantly. They also reinforce the need for organizations to adopt international frameworks like ISO/IEC 27001 and ISO/IEC 27701 to demonstrate a systematic approach to data security and privacy. Over time, the cumulative impact of such breaches may lead to higher regulatory penalties for non-compliance, stricter breach reporting timelines, and expanded rights for data subjects. Ultimately, Trinity Health's experience illustrates how a single incident can contribute to a broader push for global regulatory harmonization aimed at improving the protection of personal data across borders.

Summary

Analyzing the Trinity Health data breach demonstrates how the application of cyberlaw principles confidentiality, integrity, availability, and accountability guides organizations in managing legal, ethical, and operational risks. Here, gaps in continuous monitoring, incident detection, and communication with patients led to both regulatory exposure and a loss of public trust. By assessing these failures through the lens of HIPAA requirements, Federal Trade Commission guidelines, and international standards like GDPR and ISO frameworks, it becomes clear how legal compliance and ethical responsibility are

deeply connected.

This analysis also highlights the broader societal and cultural impacts of data breaches, such as patient reluctance to share health information and global skepticism toward digital health solutions. Reflecting on this case reinforces why organizations must not only meet the minimum legal requirements but also proactively adopt industry best practices and external standards to protect those they serve. Ultimately, applying cyberlaw principles in a practical, forward-looking way helps organizations like Trinity Health build a stronger security posture, respond effectively to incidents, and maintain the trust essential for delivering quality care in an increasingly connected world.

Citations

Alder, S. (2023, June 15). 21,000-record data breach sparks Trinity Health class action lawsuit. HIPAA Journal.

<https://www.hipaajournal.com/21000-record-data-breach-sparks-trinity-health-class-action-lawsuit/>

Federal Trade Commission. (2016, October 2). Protecting personal information: A guide for business. Federal Trade Commission.

<https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>

U.S. Department of Health & Human Services. (2024, July 19). HIPAA for professionals. HHS.gov.

<https://www.hhs.gov/hipaa/for-professionals/index.html>

ProWritingAid - the best grammar checker, style editor, and editing tool in one package. (n.d.).

Prowritingaid.com. <https://prowritingaid.com/>

MyBib Contributors. (2019, May 26). APA Citation Generator – FREE & Fast – (7th Edition, 2019).

MyBib. <https://www.mybib.com/tools/apa-citation-generator>