**Laws Influencing Information Security and Privacy in the Healthcare Sector**

Naraniya Mamatha Nagpuria

University of The Cumberlands

2024 Fall - Legal Reg, Compliance, Invest (ISOL-633-M50) - Full Term

Dr. Roger Finnegan

October 27, 2024

**Abstract**

This paper describes the complex legal structure of information security and privacy in the U.S. healthcare industry and assesses the impact of HIPAA and related laws on healthcare operations. Taking UnitedHealth Group as a model healthcare organization, this research explores the compliance strategy of an organization that works to protect sensitive information, criminal and tort risks facing an organization as a result of handling protected medical information, and its experience with forensic investigation after data breaches. The paper further examines the IP portfolio of UnitedHealth, taking a closer look at its patents and trademarks in the context of a competitive healthcare landscape. Finally, the paper assesses how the legal system both benefits and burdens healthcare organizations in their pursuit of an optimal balance of compliance, operational efficiency, and innovation.

**Laws Influencing Information Security and Privacy in the Healthcare Sector**

The digitization of health brought strong regulations concerning the protection of sensitive patient information and data privacy. Laws such as HIPAA and the HITECH Act have streamlined cybersecurity risk and confidentiality of patients in the U.S. healthcare industry in the right direction. The paper reviews how such laws impinge upon UnitedHealth Group's operations and its challenges in navigating criminal, tort, and intellectual property issues. More emphasis will be given to HIPAA-related compliance, investigation of breaches, and their aftermath on the business model of the organization.

**Laws Governing Information Security and Privacy in Healthcare**

Health Insurance Portability and Accountability Act of 1996 is the foundational law from which information security and privacy rules originally emanated for the U.S. healthcare system. HIPAA Thomas P. regarding standards to protect PHI through the Privacy Rule, in concert with the Security Rule that requires covered entities such as health insurers, hospitals, and clinics to protect patient data. While the Privacy Rule relates to the use and disclosure of PHI, such health information shall only be disclosed under legal conditions or upon consent by the patient. On its part, the rule on security prescribes certain administrative, physical, and technical controls to safeguard electronic PHI against unauthorized disclosure or modification, with the intent that sensitive information shall only be disclosed to or modified by authorized persons (Choi et al., 2006). These regulations are, then, imposed through the U.S. The U.S. Department of Health and Human Services can issue fines through its Office for Civil Rights or other penalties due to non-compliance.

Complementing HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act has, since 2009, extended the legal requirements of data breach notification and added to the potential penalties when the law is violated. It incentivized the adoption of EHRs and strengthened privacy protections in order to respond to the increased cybersecurity risks from digital data exchange. HITECH requires healthcare providers and their business associates to notify breaches of unsecured PHI within 60 days of discovery (Yaraghi & Gopal, 2018). Collectively, HIPAA and HITECH provide the backbone for healthcare information security through a set standard that reduces occurrences of data breach while cultivating a culture of accountability throughout the healthcare industry. Even with these in place, compliance challenges persist due to the addition of new technologies, such as telemedicine and cloud computing, to the complexity of data management systems (Bassan, 2020).

**UnitedHealth Group: Overview and Challenges**

UnitedHealth Group is one of the biggest health care organizations in the U.S., providing its services through two main sets of business platforms: UnitedHealthcare, purely involved with health insurance coverage, and Optum, focusing on health services and technology. UnitedHealth, due to its nature, was subject to HIPAA jurisdiction, handling volumes of Protected Health Information (PHI) so huge that it would be placed under vigorous scrutiny in terms of compliance with the call for privacy and security regulations. The organization has to ensure not only compliance with the requirements of HIPAA but also with the HITECH Act that extends breach notification conditions and penalty methods because the conflicts are more serious in their consequences (Mohammed et al., 2015). UnitedHealth, being an organization of this size and nature of operations, very frequently communicates and shares information with other covered entities and business associates, which makes it more vulnerable for the regulatory controls. There is, therefore, the need for UnitedHealth to incorporate proper technical, administrative, and physical security controls in the course of ensuring HIPAA compliance amidst the smooth delivery of health care (Mbonihankuye et al., 2019).

In spite of best efforts by UnitedHealth, this organization too has major cyber threats—such as ransomware attacks and phishing schemes—that compromise PHI and subsequently lead to legal consequences. Medical data has a high value, making healthcare organizations an attractive target for hackers who can exploit this information for insurance fraud or identity theft. Regulatory non-compliance may result in fines, lawsuits, and reputational damage (VanHoy, 2021). UnitedHealth also risks tort incidents, with possible lawsuits from patients whose data might be exposed in the event of a breach. Besides this, there are major costs in compliance maintenance—a line of employee training, system audits, and constant security upgrades. These challenges only underscore the delicate balance UnitedHealth is likely trying to achieve between operational efficiency and maintaining the level of privacy compliance for the protection of its patients and its business interests (Choi & Williams, 2021).

**Criminal and Tort Risks Faced by UnitedHealth**

UnitedHealth is at risk of criminal liabilities concerning data breach incidents on both direct and indirect violations under the HIPAA and HITECH regulations. Criminal liabilities arise due to wilful negligence or intent to compromise PHI. Based on the level of wrongdoing, a healthcare organization may be fined up to $1.5 million in cases of intentional misconduct, and even imprisonment is liable in respect of individuals involved. These risks also heighten with the increasing frequency of ransomware attacks against healthcare entities. In general, ransomware attacks lock critical systems until a payment is made to gain access, which further disrupts the delivery of care and may expose patient data (VanHoy, 2021). UnitedHealth must also adhere to breach notification rules or timely public disclosure of breaches, which is further exposing the organization to both regulatory scrutiny and reputational harm.

From a tort liability perspective, UnitedHealth's tendency is to end up in court by patients and consumers as if the breach of data results in unauthorized disclosures of personal information. Individuals alleging negligence, emotional distress, and fiscal loss in a case of unauthorized disclosure of PHI can sue. Such lawsuits will be filed at considerable costs regarding fiscal settlements and legal fees. For example, in case UnitedHealth fails to take proper cybersecurity measures, it can also be sued on grounds of negligence by the affected patients in a class action. Several recent studies seem to show that the causes of most breaches in health care happen due to preventable errors in password management or some other form of phishing, meaning thereby that chances of tort claims on grounds of negligence may increase henceforth (Yaraghi & Gopal, 2018). In addition to this, the financial implications of these lawsuits can creep beyond direct settlements into reputational damage, erosion in consumer confidence, and higher regulatory scrutiny, which will further hurt UnitedHealth's operations and profitability.

**Forensic Investigation: UnitedHealth Data Breach Incident**

In February 2024, the technology unit of UnitedHealth Group, Change Healthcare, was in the way of a ransomware attack that exposed personal data of approximately 100 million individuals. The situation is described as the largest data breach in healthcare history to occur in the U.S., surpassing the Anthem breach in 2015 involving 79 million individuals (iTnews, 2024). This included disruption of claims processing to patients and providers across the country. UnitedHealth reported it began notifying those affected in June 2024 because federal notification requirements by the Department of Health and Human Services were met. Preliminary investigations indicated the data stolen may include member insurance IDs, treatment information, billing codes, diagnoses, and Social Security numbers.

The intrusion was blamed on the hacking group ALPHV, also referred to as "BlackCat." The group succeeded in breaching Change Healthcare's systems and spurring a forensic investigation into the extent and causation of the attack. The forensic experts established the key attack vector used by the attackers to be ransomware, which encrypted the critical systems and subsequently caused healthcare operations to get paralyzed in the U.S. as a whole (Mishra & Siddiqui, 2024). In the process of forensic investigation, the investigators tried to contain the attack, restore the affected systems, and trace the vulnerabilities utilized by the hackers. This long-drawn investigation, which is still ongoing at the time of this report in October 2024, has unraveled the sophistication that is involved in the cyberattack and also brought out the requirements for more advanced security infrastructure in hospital networking.

The financial consequence for UnitedHealth due to the breach is incredibly large, as the company projects a loss of about $705 million USD, considering the disruption in the payment systems, loan disbursements to the affected providers, and compliance costs arising out of the breach notifications (iTnews, 2024). Apart from the direct monetary penalties, the breach has further dented patient confidence in the adequacy of the current cybersecurity framework for health. Response by UnitedHealth included intensifying security protocols, including staff cybersecurity awareness training and investments in state-of-the-art encryption technologies, in order to make sure such incidents do not happen again. Although the investigation into the breach is incomplete, yet again, it puts in the spotlight the pro-active approach to cybersecurity and compliance with federal data protection laws such as HIPAA and the HITECH Act.

**Intellectual Property Rights at UnitedHealth Group**

Through active management, UnitedHealth Group maintains an array of intellectual property assets, including a wide range of patents, trademarks, and proprietary technologies supporting the operations of the entity across insurance, healthcare services, and digital platforms. It also holds patents on new technologies in healthcare data analytics, artificial intelligence in health management, and virtual telemedicine solutions. These enable UnitedHealth to provide advanced care management tools and personalized healthcare services that improve both patient outcomes and operational efficiency. The investment by UnitedHealth in digital health reflects the growing trend in the healthcare sector, where intellectual property plays an important role in maintaining competitive advantage (WIPO, 2023). Securing patents for healthcare technologies ensures that UnitedHealth can control the use of these innovations and block competitors from replicating or benefiting from its research investments.

Apart from the patents, UnitedHealth has a number of other trademark filings to help protect the brand identity for subsidiaries and service brands such as Optum and Change Healthcare. Trademark protection helps the company nurture consumer trust and brand recognition in a competitive healthcare environment where separation is critical. Proper IP management also shields UnitedHealth from risks of infringement. If any entity uses its proprietary tool without permission, a legal fight may ensue. The fact that UnitedHealth might not have its proprietary algorithms and analytics misused or stolen should certainly stand out with the increasing trend of healthcare companies adopting data-driven approaches (Goldenberg & Grantcharov, 2018). Therefore, IP management coupled with compliance with the regulation of healthcare data will enable UnitedHealth not only to maintain its leading position in the market but also to continue further developments within such a highly regulated and technologically dynamic industry.

**The Impact of the Legal System on UnitedHealth Group**

The establishment of laws like HIPAA and the HITECH Act creates a challenge and an advantage in the legal framework of health data privacy for UnitedHealth Group. It provides a standard procedure to be followed by the organization in safeguarding PHI, thus helping in gaining the trust of the patients and providers by complying with these regulations. Complying with the federal regulations also diminishes the possibility of receiving harsh fines for data breaches, showing good faith in attempting to protect sensitive information (Yaraghi & Gopal, 2018). Multi-factor authentication and encryption of data with perquisite usage under HIPAA enable the minimization of vulnerabilities. It does, however, take a great deal of monetary investment in technology and employee training to remain compliant with the ever-evolving set of regulations and thus can be very overwhelming to a company the size of UnitedHealth (Mbonihankuye et al., 2019).

While this may be so, the legal requirements at the same time make it difficult for operations to implement new technologies because of the concern about their compliance with regulations. For instance, the ongoing digitalization within this sector depends on the accelerated renewals of technology; yet, the need to develop novel systems based on privacy legislation, such as that regarding the UnitedHealth case, has a negative effect on the trendiness and ease of such implementations (VanHoy, 2021). In addition, the legal system imposes breach notifications within specific time limits, increasing the burden it imposes on firms to remain open, in cases such as the breach that involved UnitedHealth because of the ransomware attack that its Change Healthcare unit faced in 2024. While, in general, regulatory frameworks provide a way to secure data, the financial and operational burden of maintaining compliance remains a critical challenge to healthcare organizations. The challenge for UnitedHealth is balancing this legal obligation to do so, on the one hand, with the need for innovation and operational efficiency on the other hand.

**Conclusion**

Legal factors have a central role for universal health care organizations such as the UnitedHealth Group since they act to guide all its operations. Nevertheless, laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology and Clinical Health Act (HITECH) protect the patient’s delicate information but also add to the problem of increased compliance and operational cost. UnitedHealth's experience with data breaches and forensic investigations has raised awareness about the importance of robust cybersecurity measures and adherence to legal standards. The effective management of their intellectual property is another strong point of this organization that has kept it competitive in the market. In a nutshell, there are adequate legal regulations of healthcare privacy and security to maintain rights and proper defense of patients as well as organizations. But it is important to understand that to get compliant, one needs to balance data protection, operational performance, and innovation. As seen from UnitedHealth’s experience, although the law may place substantial burdens, it is, in fact, effective in raising the level of reliability of actors in the healthcare industry.

**References**

Bassan, S. (2020). Data Privacy Considerations for Telehealth Consumers amid COVID-19. *Journal of Law and the Biosciences*, *7*(1). https://doi.org/10.1093/jlb/lsaa075

Choi, Y. B., & Williams, C. E. (2021). A HIPAA Security and Privacy Compliance Audit and Risk Assessment Mitigation Approach. *International Journal of Cyber Research and Education*, *3*(2), 28–45. https://doi.org/10.4018/ijcre.2021070103

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules. *Journal of Medical Systems*, *30*(1), 57–64. https://doi.org/10.1007/s10916-006-7405-0

Goldenberg, M., & Grantcharov, T. (2018). Enhancing Clinical Performance and Improving Patient Safety Using Digital Health., 235-248. <https://doi.org/10.1007/978-3-319-61446-5_17>

Goldstein, M. M., & Pewen, W. F. (2013). The Hipaa Omnibus Rule: Implications for Public Health Policy and Practice. *Public Health Reports*, *128*(6), 554–558. https://doi.org/10.1177/003335491312800615

iTnews. (2024, October 25). *Hack at UnitedHealth’s tech unit impacted 100 million people*. ITnews. https://www.itnews.com.au/news/hack-at-unitedhealths-tech-unit-impacted-100-million-people-612616

Mbonihankuye, S., Nkunzimana, A., & Ndagijimana, A. (2019). Healthcare Data Security Technology: HIPAA Compliance. *Wireless Communications and Mobile Computing*, *2019*(1), 1–7. https://doi.org/10.1155/2019/1927495

Mishra, M., & Siddiqui, Z. (2024, April 22). *UnitedHealth says hackers possibly stole large number of Americans’ data*. Reuters. https://www.reuters.com/technology/cybersecurity/unitedhealth-says-hack-could-impact-data-substantial-proportion-americans-2024-04-22/

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector. *International Journal of Business and Social Research*, *5*(2), 55–66. https://doi.org/10.18533/ijbsr.v5i2.714

Team, S. (2024, September 26). *United Healthcare Data Breach Explained (How to Prevent It)*. Strongdm.com; StrongDM, Inc. https://www.strongdm.com/what-is/united-healthcare-data-breach

VanHoy, J. (2021). Healthcare Sector Security Analysis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3763392

WIPO. (2023). *The Digital Health Revolution: Leveraging Intellectual Property for Equitable Access and Innovation*. Global-Health. https://www.wipo.int/web/global-health/w/news/2023/news\_0011

YARAGHI, N., & GOPAL, R. D. (2018). The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study. *The Milbank Quarterly*, *96*(1), 144–166. https://doi.org/10.1111/1468-0009.12314