Code Blue: Legal Issues for Healthcare Cybersecurity Incidents

Danielle Caplinger

College of Interdisciplinary Studies, Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Professor Tucker

March 4, 2025

Code Blue: Legal Issues for Healthcare Cybersecurity Incident

With technology evolving at an unprecedented rapid pace, it comes as no surprise that these advancements have been used in the medical industry in order to become more efficient and improve patient lives. Unfortunately, as technology becomes so ingrained in any industry, these industries open themselves up to facing the security concerns that come with such technologies. In the wake of this phenomenon, it is important to understand what cybersecurity concerns exist in the healthcare industry on a technical level. Additionally, legal experts must explore privacy concerns and legal ramifications for cybersecurity breaches in the healthcare industry. Finally, medical professionals focus on how these technologies, and their security concerns, affect their patients health and even their lives. A solution must be found to this issue where cybersecurity incidents in the healthcare industry are increasing with potential for human lives lost without any legal clarity on potential liability.

Interdisciplinary Justification

Given the complexities of this topic, a singular disciplinary approach would not be sufficient to fully comprehend the problem or develop viable solutions. To truly understand the privacy issues regarding the healthcare industry's cybersecurity incidents, all perspectives must be thoroughly examined using the interdisciplinary research process. To that effect, this research focuses on the disciplines of technology, health sciences, and law to create a comprehensive approach to mitigating this problem as it becomes increasingly prevalent. The interdisciplinary research process is a ten-step model that guides interdisciplinary research from a problem to a better understanding of the topic through insights and integrating these insights (Repko & Szostak, 2021, p.76). This paper will first focus on a literature review from the aforementioned disciplines to identify relevant concepts and potential relationships between perspectives.

Particular focus will be drawn on common ground that can be used to identify solutions to this problem. In order to properly incorporate ideas, horizontal integration was used to effectively explain the relationships between disciplines, the underlying problem, and potential solutions.

Literature Review

Existing literature regarding medical technologies involved in cybersecurity incidents, breaches, or other events is minimal as most are specific to the affected device, organization, or type of information. Nevertheless, technologists studying the issue tend to divide their views into two categories: those focusing on the specific attack possibilities that the healthcare industry allows for, and those focusing on vulnerabilities in the healthcare industry that allow for such attacks to take place. As with any technology, medical technologies are susceptible to a variety of attacks including, but not limited to: information breaches, command and control attacks, denial of service attacks, and compromises using malware. According to Williams and Woodward, however, there are additional factors for medical devices because "these devices expose both data/information and potentially the control of the device itself" (Williams & Woodward, 2015, p. 308). The attack surface of medical devices poses significant challenges because these attacks can directly affect human lives. As researched by Alexander and his co-researchers at Queen's University, there are already some examples of malicious attackers remotely tampering with the amount of insulin that an IoT-connected insulin pump administers, potentially causing hypoglycemia in diabetic patients (Alexander et al., 2019, par. 1). As evidenced by this, there is an increased awareness of specific attack surfaces that cybersecurity professionals must be aware of in order for technology to be secure enough for medical use.

Technologists also have a focus on research regarding the vulnerabilities in medical technology and medical systems that do not necessarily exist elsewhere. Vulnerabilities are

generally considered to be any weakness in a system that allows a cyber attack to take place. Medical systems, by their very nature, are meant to be secure to protect patient confidentiality, but there is no such thing as an impenetrable network or system. To account for this, a strong cybersecurity posture almost always includes strong patch management, a system where updates are installed based on a predefined measure of frequency and severity. Williams and Woodward posit that interoperability between devices and manufacturers, which is common in hospitals and other medical settings, act as "a major confounding factor" because they require "a secure configuration of the network and attached [medical] devices" that don't necessarily allow for optimal patch management (Williams & Woodward, 2015, p.311). This comes from the fact that medical devices are difficult to manage from an update management standpoint because of their physical location or lack of regular connection to the larger network. Some researchers emphasize that patients should be involved in that process "given the possibility of adverse events with both accepting and not accepting the firmware upgrade" of their medical devices (Alexander et al., 2019, par. 9). There are also increased vulnerabilities in these medical devices because of the existing years-long process from conception to implementation in patients where multitudes of vulnerabilities can "be discovered in the implanted lifetime of many devices" (Alexander et al., 2019, par. 17). All of these factors create intense cybersecurity issues where vulnerabilities can be exploited at a much faster rate than can be effectively mitigated.

Compared to technologists, there is not much specific literature from medical professionals regarding how medical professionals can address this issue. However, the underlying theme is that they must be aware of cybersecurity impacts in healthcare as long as it does not undermine patient care. Clinicians do not have the technical capabilities to create or secure their systems, but they still face the challenge of making sure they are secure enough to

protect their patients. Otherwise, it "can erode patient trust, which is fundamental to the clinician-patient relationship" (Elendu et al., 2024, p.22). Elendu highlights, however, that a medical professional's "goal is not to create barriers" but to make sure that protections against healthcare data won't "impede healthcare delivery" (Elendu et al., 2024, p.9). Another medical researcher, Alanazi, proposes a differing relationship where medical professionals' "drivers for cybersecurity are gaining patient trust and enhancing the hospital's reputation" (Alanazi, 2023, p.6). This creates a reliance on cybersecurity professionals from clinicians in order to best protect their patients. As a whole, health professionals are acting as an intermediary to fulfill their role as protector and keeping patient care at the forefront of decision-making.

Given that the legal system is years behind current events, existing literature regarding medical privacy laws and liability in the digital age is relatively vague and outdated. To this point, a legal professor, Silverman brings up that courts repeatedly use common language of "'reasonably designed' and 'comprehensive' privacy and data security measures" rather than mentioning any specifications that would meet this requirement (Silverman, 2018, p.217). This language is seen regarding any data breach, but he specifically mentions this in the case of LabMd, Inc. v. FTC where medical data was at risk. Silverman offers an alternative to this vague language where "court[s] must look at all of the available facts" when "assessing the risk of future harm… [regarding] the breach. [This involves] informed deductions about why the information was taken, and what might be done with it in the future" (Silverman, 2018, p.219). By doing so, liability can be appropriately correlated based on if security controls were grossly negligent or simply weak against an unexpected attack. This proposal would work for medical information breaches as well as medical device liability cases. The other prominent legal perspective regarding the healthcare industry is regarding HIPAA, the Health Insurance

Portability and Accountability Act. As with other legislation, it is becoming increasingly outdated especially considering "the health information industry has transformed leaving substantial gaps between advancements in digital health and privacy laws" (Theodos & Sittig, 2020, p.7). As of now, there are still no specific requirements to make medical systems and data secure against cybersecurity incidents, although proposals have been made. Legal researchers are calling for more specific regulations regarding this, especially considering the anticipated rise in lawsuits regarding healthcare cybersecurity breach liability, but are wary of the legal system never truly catching up to technological advancements.

Applications

These three disciplines may appear to have contradicting motivations when it comes to addressing the liability issues in healthcare cybersecurity breaches. As seen earlier, technologists are concerned about making their networks and devices as secure as possible. On the other hand, medical professionals want patient care to remain forefront in their minds by safeguarding their patients' trust and health. Finally, legal professionals focus on the lack of existing, specific legislation that both regulates and settles cases regarding medical privacy and liability issues. Despite what seems to be contradicting perspectives, there are a multitude of similar themes and insights that can be found to help solve this issue. To formulate an appropriate solution, common ground needs to include: patient safety, the future of technology, and a liable entity. By exploring these concerns with an interdisciplinary perspective, a solution can be proposed that addresses every aspect of the complex problem of healthcare cybersecurity breach liability.

As expected, patient safety is a primary concern when the healthcare industry is involved. Interestingly, this sentiment is not just shared by medical professionals, but cybersecurity and legal professionals as well. Medical professionals, as discussed previously, must act with their

patients best interest, and more importantly, health in mind. It is because of this role that they become involved in making sure that the systems and devices used are secure. Cybersecurity professionals get involved at this stage in order to provide the technical expertise needed to fulfill this objective. Although technologists are aware and mindful of the increased attack surfaces and vulnerabilities that medical systems create, this does not necessarily mean that these technologies should not be used. In fact, a key tenet of cybersecurity is making sure that technology is accessible and available when it is needed. To further that, cybersecurity professionals in this role must make sure that technology is available so that patient lives can be improved while making sure it is secure enough to not endanger it. Legal professionals come into play here because their stake is in making sure that laws and regulations act as a guide to protect patient lives. Lawyers in particular need this precedent in the event that a breach of privacy or even tangible harm is done based on a cybersecurity incident so that the proper persons are held accountable for any harm done to the patient.

There are also similar paths to consensus when it comes to the future of technological advancements in the medical industry. As with many technologies, medical technologies are advancing at an unprecedented rate. More and more conditions are being treated using technologies as a tool or physically implanted into the body. This is the main reason that medical professionals are advocating for this advancement to continue and more patient lives to improve. Additionally, protected health information is expanding to include more data fields that are becoming accessible by multitudes of networks. A cybersecurity perspective notices how this opens up even more potential opportunities for breaches, hacks, and other incidents. However, this also allows for more advancements in cybersecurity defense and protections that can be used to mitigate these threats. Because of this, legal experts are also proponents of technological

advancements as long as the proper mitigations are in place and acceptable legal consequences for not using standardized practices are created in some capacity.

At the core of this issue is the obscurity of who the liable party would be if a cybersecurity incident were to occur in the healthcare industry. Existing laws and regulations do not answer this question with any clear certainty. Instead, similar legislation tends to align itself with whomever was the most responsible for the incident occurring. In most cases, this would be the attacker or group that infiltrated a network and stole data or misused the device. However, negligence plays a role here in cases where the technology fails without interaction with an attacker or when standard practices to keep attackers out are not followed. This potential negligence creates dubious precedent for lawyers on either side of a potential case on who is most responsible for damages, fines, or other harm. Medical professionals are also worried about this unknown liability factor and looking for clearer guidelines. This includes malpractice concerns regarding prescribing or recommending medical technologies that could potentially be harmful if an incident is to occur. Cybersecurity professionals are also concerned regarding if they could be liable if an insecure network or device could be the potential defining factor in a liability case. This is important as there is no way to completely secure any network or device, creating more risk for cybersecurity professionals when accounting for liability.

Recommendations

By integrating these disciplines together and subsequently finding the common concerns for this problem, it is now possible to address the issue appropriately and solve some aspects of it. Given the case-by-case nature of a liability case, a completely universal answer cannot be given at this time. Nevertheless, guidelines can be set by the appropriate parties and certain approaches can be implemented to minimize potential cybersecurity incidents. A key aspect of

these guidelines being successful, however, comes from the appropriate parties being involved in setting such recommendations. Since the main parties involved come from cybersecurity, medical, and legal professions, these same disciplines should be involved in creating these guidelines. Additionally, these recommendations should be regularly reviewed and potentially updated in order to stay as up-to-date as possible.

Included in these guidelines would be best practices for keeping digital information, including private health information, as secure as possible. Standard data security would apply here including encryption, access control, and version control. Regarding medical devices, guidelines should, at their inception, refer to regulations put forth by medical associations, legal agencies, and manufacturers of such products in use. Other standard cybersecurity practices including patch management, regular updates, and vulnerability management systems should be applied to previously installed devices where it will not cause patient harm. That being said, new medical devices should be made with a secure-by-design process where security is built into the device in the event that they cannot necessarily have improved security through the rest of the device's lifetime. Medical professionals can contribute to this process by making sure that they are only using systems and recommending devices that follow such guidelines in the name of keeping patients safe. This creates more clarity for legal professionals to assign negligence or liability based on the party ignoring such guidelines.

Conclusion

Finding an effective solution to liability issues arising from cybersecurity issues in the healthcare industry is not a simple task, nor can it be done by a single discipline. By examining the goals and objectives of cybersecurity, medical, and legal professionals, it becomes possible to put forth a proposal for guidelines that could help resolve some of this issue. As with most

technological issues in the modern era, there will not be a clear and concise solution that fits every situation. However, with the correct parties involved and their adequate diligence in working towards their shared purpose, it can be improved. As all three of these disciplines share the common goal of patient safety in a future of unprecedented technological medical advancement and regulation, it is important that research does as well. Without it, patient lives could be lost, laws will remain unwritten, and society will remain stagnant.

References

Alanazi A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus, 15*(10), e47026. https://doi.org/10.7759/cureus.47026.

Alexander, B., Haseeb, S., & Baranchuk, A. (2019). Are implanted electronic devices hackable?. *Trends in cardiovascular medicine*, *29*(8), 476–480. https://doi.org/10.1016/j.tcm.2018.11.011.

Elendu, C., Omeludike, E. K., Oloyede, P. O., Obidigbo, B. T., & Omeludike, J. C. (2024). Legal implications for clinicians in cybersecurity incidents: A review. *Medicine*, *103*(39), e39887. https://doi.org/10.1097/MD.0000000000039887.

Repko, A. F. & Szostak, R. (2021). *Interdisciplinary Research: Process and Theory* (4). Sage Publications.

Silverman, D. L. (2018). Developments in Data Security Breach Liability. *The Business Lawyer*, *74*(1), 217–228. https://www.jstor.org/stable/27171170.

Theodos, K., & Sittig, S. (2020). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. *Perspectives in health information management*, *18*(Winter), 1l. https://pmc.ncbi.nlm.nih.gov/articles/PMC7883355/.

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.)*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048.