JS|HELD

PERSPECTIVES

Inside the Healthcare Industry: Understanding Evolving Data Privacy & Artificial Intelligence Security Risks and Regulations

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Data privacy and security threats are impacting all aspects of the healthcare industry – from providers to payers, to medical device companies, to clinical decision support software companies, and further down the line, according to the Theft Resource Center. These events have far reaching ramifications – for consumers, their patient privacy and personal information is at risk, and for healthcare companies much is at stake, from impacts on their ability to operate, to erosion of consumer trust, to strength of their bottom line, and vulnerability to government investigations and litigation.

Given all of this, it comes as no surprise that there are growing (and evolving) regulations that govern how healthcare organizations protect their data. There are significant changes proposed for the HIPAA regulations. On December 27, 2024, the HHS Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) aimed at significantly updating the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, originally established in 2003 and last revised in 2013.

This proposed overhaul comes in response to the evolving healthcare landscape, increased cybersecurity and privacy-related concerns, and insights gained from both law enforcement and subject matter experts. The current draft covers a number of key updates, including mandatory encryption of ePHI (electronic Protected Health Information), annual compliance verification, robust risk management, asset inventory and network mapping, and clearly defined incident / response plans within 72 hours of an incident, among other provisions. These updates impact nearly all healthcare companies.

In this Q&A conversation, healthcare expert Magi Curtis, and Digital Investigations & Discovery experts George Platsis and Antonio Rega, discuss the intersection of cybersecurity and data privacy with government regulation as it applies to the healthcare industry.

Magi: We have seen a lot of action on the data privacy and security fronts with our clients and law firm partners lately. Having worked with healthcare executives for years, I've heard first-hand from countless general counsels that data privacy, security, and cybersecurity are among the top issues that keep them awake at night. Given that this is a trend that is only likely to intensify, I would love to know what both of you – data privacy and cybersecurity experts – are seeing that most affects our healthcare clients.

George: There is so much data being created. Not only on a mass scale, but personalized individual level data. This data is being created everywhere. It is generated not only when you go to a hospital, having your images done, or getting routine work from your healthcare provider; a consumer can generate input data into a system right now all on their own through a personal device, whether it is an oxygen level or a blood pressure monitor. All of that can be done via Bluetooth, wireless, wearable, and internet-enabled technologies. Health data is generated from you, moves to your phone, and then from your phone, it goes to an app.

It begs the question: where is all that data going afterwards? Moreover, can you validate that the data is going – and staying – where it is supposed to? And after that, what confidence do you have that the data is secure? And what is being done with that data? These are open-ended questions, and few can answer them with absolute certainty. The fact that we continue to see breaches and leaks illustrates that these questions remain unanswered.

Antonio: An issue that I'm seeing a lot is the amount of information and data that's being collected, stored, and potentially transferred to third parties or even back to a healthcare organization's infrastructure, such as through unsecured remote access. On this issue, the biggest question that healthcare companies should be asking themselves is what sort of safeguards do they have in place? Protected health information (PHI), especially in the healthcare industry, is of paramount importance. Healthcare companies are vulnerable to potential HIPAA violations if they're not safeguarding health information and other types of personal information properly. This is true particularly when we're talking about mobile devices and apps. There are so many apps out there now that are recording and storing health information.

Third-party tracking technology has been a hot topic in the last couple of years and it opens up healthcare organizations to compliance issues and litigation. Although the American Hospital Association (AHA)

won their lawsuit that required HHS and the Federal Trade Commission (FTC) to roll back newly imposed online tracking technology restrictions, privacy-related challenges still remain.

Of note, Meta has introduced new data-sharing restrictions for regulated industries, including healthcare, in 2025. These changes could significantly impact how businesses use tools like Meta's tracking pixels and other related measures utilized by organizations for marketing purposes. This action is due in large part to increased lawsuits, regulatory complexity, and (negative) public sentiment directed at companies offering these types of marketing tools, particularly as it pertains to PHI.

Additionally, the HHS Office for Civil Rights (OCR) has been actively updating its guidance on how HIPAA applies to the use of online tracking technologies, though the guidance was later vacated by a US District Court in June 2024, and discussions currently remain ongoing. That aside, given the ongoing security and privacy concerns around this topic, there's an anticipation that regulatory bodies will be sharing updated guidance in 2025, which should incentivize healthcare-related entities to remain vigilant.

George: In addition to the challenges posed by tracking technology, healthcare organizations should be mindful of the constant threats to data, regardless of the source. One area where we see increasing risk is through third-party relationships, as they often represent a critical dependency for service delivery, or in some cases, even a weak point, giving malicious actors access into multiple organizations all at once. The types of third-party services that are prime targets include technology providers, managed services, cloud and data storage providers, and application and productivity software. The net impact of these dependencies is that a successful attack can cascade across multiple entities.

Magi: Given all of this, how should healthcare executives be thinking about preparing now so that they can protect their organization, their data, and the information of those they serve?

George: Boards and executives should be mindful of the ever-changing cybersecurity risk management rules, such as those issued by the US Securities and Exchange Commission, the Cyber Resilience Act of the European Union, or the multiple US state laws being issued. For example, the SEC rules require oversight of cybersecurity risk, along with demonstrable evidence of management's role and expertise to manage cyber and data risk. Issues to consider include disclosure requirements of cybersecurity incidents on Form 8-K and the concept of materiality. And while the SEC rules only apply to public companies, privately held companies would be wise to consider implementing practices that align with the rules.

Antonio: As I mentioned earlier, while the win by the AHA against the HHS in regards to the use of tracking technology aided in minimizing government overreach as claimed in the lawsuit, litigation on this issue remains ongoing. For example, in states like California, which has the California Consumer Privacy Act (CCPA) in place, there continue to be legal claims alleging that the use of cookies and pixels on websites violate provisions of the California Invasion of Privacy Act (CIPA). However, it should be noted that there have been recent wins for defendants in these cases.

As litigation continues in tracking tech-related matters, while guidance has been softened, the need for proper management of personal and protective health information persists for healthcare organizations. This underscores the need for key stakeholders (compliance and legal, privacy and IT security teams, etc.) to assess the security and privacy provisions in place for applications, medical devices, or even website content. One approach can be to set up internal working groups and committees that can talk through this and establish clear frameworks for handing personal identifiable information (PII) and protected health information (PHI). Also, they should make sure there are business associate agreements (BAA) in place for third-party platforms they're utilizing.

George: On a more macro level, healthcare organizations need to determine what their risk tolerance is and what factors should be considered in calculating that risk tolerance. Is it just patient care? How does data handling change that risk level? And how about

financial risk? Anything else? Each organization has different factors to consider. Due to the issues raised, newer risks are becoming increasingly more difficult to quantify.

For example, an organization could potentially quantify patient harm. They could even quantify financial interruption to a certain extent. But fines or potential fines from the SEC, or some other body, or reputational damage caused by an incident, are factors that are harder to quantify. You almost have to consider a worst-case scenario and work backwards from that, but many organizations shy away from doing that, which could end up undershooting their risk tolerance and calculations. That is why this exercise is both art and science. Think of the downstream impacts of a data leak, as an example. The costs do not end once the leak has been remediated. That is still the start. Organizations must consider things like ongoing costs of monitoring services or class action suits that could potentially come down the pipeline. Do the risks outweigh the benefits of having all this data generated out there across multiple systems and platforms? My sense tells me, as time passes, the answer may be, no.

Organizations should also be talking about the use of artificial intelligence (AI), because of its privacy and security implications. AI may be partly a misnomer. Currently, AI is trending towards machine learning. So far, we have seen that machine learning can be very beneficial in healthcare, but equally unreliable depending on the use case.

Antonio: Good points. I would add that technology like generative AI, which is a type of large language model (LLM) has its limitations and remains subject to a somewhat crude legacy phrase: "garbage in, garbage out," or put another way: the quality of data input governs the accuracy and reliability of the data output. There are a number of key risk areas, such as *alignment* issues (i.e., what you may expect a certain AI model to generate versus what is actually generated may not necessarily be in *alignment*). As such, consideration should always be given to how reliable the information is, and to what extent the output is being vetted and / or corroborated. And finally, with regard to AI, just like all other data, healthcare executives should be looking proactively into where the aggregated information is being stored. Is it in a place that is potentially vulnerable for hacking or a breach? All that aside, there is significant upside potential in implementing AI frameworks within healthcare organizations when properly maintained, administered, and vetted.

Magi: I know that both of you have handled a lot of sensitive issues for healthcare clients. What are some of the thornier issues you have seen and how did you help the client to successfully navigate the challenge?

George: In my experience, healthcare delivery, specifically the technologies behind them, and security requirements do not always align. Think about it like this: is the intent to provide better healthcare or to secure information systems? It has always been the former, but the dependencies we have built into these delivery systems now require both. For example, a device manufacturer now needs to consider the information security implications if certain technologies are integrated, such as web access, or near-field radios. Moreover, these technologies may quickly go out of date or become technologically vulnerable. What is the process to correct these issues? Are devices penetration tested before they go to market? Is there a patch management plan for the device over its lifespan? These are questions that were not asked in the past but now pose real a nd present dangers.

Magi: So, what's the lesson here, George?

George: Developers should build security and update requirements into the research and development phases, a security-by-design mindset. This means that this should be done at the start of the project and reviewed at each major milestone throughout not only the development life cycle, but the reasonable life cycle of the device as well. NIST 800 -161 Special Publication Developing Cyber-Resilient Systems: A System Security Engineering Approach is a great place to start if people want to learn more about this approach.

Antonio: Two prior scenarios I will share, albeit with certain details excluded. One involved a biotech company in an intellectual property trade secret matter involving allegations against an executive who left the organization. The company claimed he took some trade secrets and patents. He said he didn't. There was

a specific date that was crucial, prior to his last day, where the company claimed he allegedly managed to make his way back into the office by saying that he had to retrieve some additional materials. He claimed he was never in the building on the day in question because he was on vacation. Unfortunately for him, he happened to have a health tracker on his mobile device, in addition to other datapoints retrieved from that day (such as key card access data). We were able to recover and extract activity that placed his geolocation specifically in that building, within his office cubicle on a specific day and time, when he claimed to be somewhere completely different. The lesson here is that information on user activity is ubiquitous. It can be utilized to inform an investigation, as exemplified here, though it may also cause potential compliance and privacy concerns, as we've indicated throughout this discussion.

In another example, we were retained to assess a healthcare app developed to facilitate remote interactions and sharing of information between patients and their doctors during telehealth meetings. We were engaged to identify any compliance-related vulnerabilities with the app. One of our discoveries during analysis of the code, identified instances where PHI and PII were not properly *anonymized*, which in turn led to follow-up with the app manufacturer about some of the coding flaws. The key takeaways for any healthcare organization that may be either building or working with outside parties to develop their own application are to ensure there is proper vetting of the underlying code, that masking or *anonymization* is properly implemented, confirm that there are proper opt-outs being employed, and also ensure that these functions are actually being executed at the code level.

George: Another thought, healthcare organizations need to seriously consider what data needs to be kept and what should be deleted or destroyed. There is a temptation to keep it, but that may not be the wisest decision. If you do not need the data, destroy it, and avoid the hoarding mentality. Be mindful, when organizations go through mergers, or technology transformations and rebuilds, data all becomes fragmented or misplaced. This is on top of all the data generation, making it difficult to know where your data is. You need to get rid of data you are not using, plan to use, or are not legally required to maintain. Data is an asset, but now it is increasingly becoming a liability.

Magi: Please pull out your crystal ball and tell us where you think the future of healthcare data security is going.

Antonio: As far as where I see things going, the continued evolution of AI, the use of cloud-based repositories, and *software as a service* – all of these things are going to be getting user information, whether it's PHI or PII. There will be more places where data will reside. Conduct those routine recurring monthly checkpoints internally to reassess where you are. Make sure that you have proper training internally. And when all else fails, if you're not sure, take it fully offline, or as George mentioned above, proactively purge content, especially if it is within legacy / outdated frameworks. Consider not using certain technology like third-party tracking tech or turning it off for a little while until you get the guidance from an expert or outside party.

George: There will likely be a temptation to adopt technologies that purport to offer better care. These technologies could include AI-augmented reality *internet of things* devices in hospitals or healthcare centers. The temptation will be too high to *not* integrate, as these technologies can fuse together multiple data streams stored in different places, accessible to multiple users, whether they are patients or hospital staff, or in the worst case, outsiders who have gained authorized access. A whole bunch of people are going to be touching a whole bunch of information through these technologies. My advice would be to resist the temptation to adopt that technology until you weigh those risks and build processes to mitigate them.

ACKNOWLEDGMENTS

We would like to thank our colleagues Magi Curtis, Antonio Rega, and George Platsis for their insights and expertise that greatly assisted this research.

MORE ABOUT J.S. HELD'S CONTRIBUTORS

Magi Curtis is an Executive Vice President and leads J.S. Held's Healthcare Sector Services. She has spent

her career in healthcare, in both the policy and business sides of the industry. She has guided some of the nation's leading health systems and provider-based organizations as they navigated enterprise level change management initiatives, strategic partnerships and post-merger integration, strategic positioning, government relations and significant issue campaigns, crisis events, and internal and external engagement efforts. She has also worked closely with the founders of emerging healthcare companies to scale their business and establish operational structures to maximize productivity and enable growth. Prior to joining J.S. Held, Magi was a partner at a top national healthcare consulting firm. Magi also worked in Washington, D.C. in health policy as a staffer in the U.S. Senate, at Navigant Consulting, and the Children's Hospital Association.

Magi can be reached at magi.curtis@jsheld.com or +1 615 626 0023.

Antonio Rega is a Managing Director who leads the data privacy and information governance team under Digital Investigations & Discovery services in J.S. Held's Global Investigations Practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, data privacy & information governance, digital assets / blockchain technology, and discovery on behalf of global corporations and law firms. Based in New York, Antonio regularly assists clients with advice and strategy through all phases of a given client need, including regulatory compliance, responses to government subpoenas, and expert testimony, when required.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 345 8502.