SQUIRE PATTON BOGGS

HealthTech Becomes the New Focus for Data Privacy and Cybersecurity Regulation & Enforcement

There is no shortage of attention on health care data privacy and cybersecurity, with an avalanche of new and proposed government and regulatory initiatives underway. Although health care has long been a key target for malicious actors given the data sensitivity and potential for life-threatening disruption, the rapid rise of health care smart devices — from fitness and portable devices to health care tracking apps — is intensifying the focus on data privacy and cybersecurity.

Over the last year, government-led reports, enforcement actions and new regulatory proposals have thrown health care technology, or health tech, into the limelight. While health care is already highly regulated, with the Health Insurance Portability and Accountability Act being one of the country's most robust privacy and security laws, there remain significant gaps that the government is increasingly seeking to fill. For example, the U.S. Food and Drug Administration announced in April their intention to seek more regulatory power over medical devices, with the launch of their Medical Device Safety Action Plan. At the same time that the House Energy and Commerce committee has begun investigating how to secure legacy devices commonly used in the health care industry.

Between the FDA, U.S. Department of Health and Human Services' Office of Civil Rights, which enforces HIPAA, the Federal Trade Commission and Congress all firmly focused on health tech, companies that, for example, produce internet-connected devices or software solutions will have to contend with a number of different regulatory priorities and government oversight. The stakes are therefore very high for health tech companies, requiring a robust approach to data privacy and security.

Regulatory Patchwork

HIPAA has long been a privacy and cybersecurity focal point in the health sector, but HIPAA does not apply to many entities, such as medical device manufacturers in most cases or consumer-driven health care apps. As one of the measures aimed at filling this gap, the FDA published draft guidance in December 2017 explaining how FDA would regulate (or not) patient and clinical decision support software, based on changes to the meaning of "devices" in the 21st Century Cures Act. This guidance supplemented preexisting FDA premarket and postmarket cybersecurity guidance for medical devices.

Most recently, the FDA announced plans in April this year to enhance device safety through, among other measures, several steps such as streamlining postmarket safety mitigation and further enhancing cybersecurity. Their plan would require manufacturers to maintain a list of third-party code used in a given device, known as a software bill of materials or SBoM, ensure patchability to allow security flaws to be effectively handled, and implement coordinated disclosure programs if a flaw or breach is discovered.

Meanwhile, OCR has issued guidance for mobile health app developers, helped develop a tool to evaluate the laws applicable to mobile health apps in connection with other agencies and developed a portal designed to provide guidance to health app developers. OCR has also been aggressive in its enforcement, which has led to significant settlements. In August 2017, CardioNet, a wireless health service provider, settled a case with the OCR for $2.5 million after OCR received two breach reports in early 2012. The breaches were allegedly the result of a somewhat common scenario — an unencrypted laptop stolen from an employee's vehicle. Like most OCR settlements, it was alleged that CardioNet failed to conduct an accurate and thorough risk assessment — a topic that OCR has recently provided guidance about in its monthly security newsletter — and failed to implement a security management process to reduce risks to a reasonable and appropriate level.

Like most settlements, OCR ended up evaluating a large swatch of CardioNet's procedures that formed the basis for the settlement as much as — if not more than — the original data breach that led to the investigation. It is therefore critical for companies to conduct an accurate and thorough risk assessment and then implement a security management process to reduce risks to a reasonable and appropriate level. It also points to the fact that policies and procedures need to actually be implemented and followed.

Not to be outdone, the FTC has also targeted privacy and security enforcement in the health sector. The FTC utilizes its FTC Act Section 5 authority to obtain comprehensive settlements relating to unfair or deceptive acts and practices relating to privacy and cybersecurity — for up to 20 years. Indeed, over two years ago, FTC began sounding the alarm on companies using consumer health data, including enforcement actions against medical billing and health record companies.

Health tech companies therefore need to be mindful of the myriad of new regulatory guidance and enforcement priorities from many different regulators.

Government Action

In addition to regulators, legislators are also focused on health tech. The bipartisan sponsored Senate Internet of Things Cybersecurity Improvement Act of 2017-18 and its companion piece of legislation in the House of Representatives looks to ensure "cyber-hygiene." Another bill — DIGIT Act S. 88 — has already passed the Senate and has now passed to the House. Reps. Darrell Issa, R-Calif., and Suzan DelBene, D-Wash., who co-chair of the IoT Caucus, have recently urged Congress to pass the bill, which would create a federal working group to develop IoT standards.

Other bills put an onus on various government departments to plan for such technology. Securing IoT Act of 2017-18, HR 1324, would require that the Federal Communications Commission establish cybersecurity standards for equipment utilizing radio frequency for the entirety of that technology's lifecycle.

The House Committee on Energy and Commerce has also prioritized this issue. The chairman of the committee last year sent a letter to the Department of Health and Human Services requesting that the department develop a plan to better address risks stemming from medical devices including the need for a SBoM, effectively an ingredients list of the device's software components. Now, the same committee is investigating legacy health care technology. In April this year, it posted a request for information regarding the use of legacy technologies in the sector, which pointed to how such technology has been the "root cause" of many incidents. It is likely that this will lead to more inquiries over the coming months and further recommendations or congressional actions.

Many of these recent developments can arguably be traced back to the government-led Health Care Industry Cybersecurity Task Force report on improving cybersecurity in the health care industry in June 2017. The report raised areas of increased focus for the industry on how best to protect systems from potential threats including recommendations to help companies improve cybersecurity resilience. Throughout its report, the task force remarked on the "cybersecurity digital divide," where larger organizations might have the resources to manage cyber risks, while smaller health care organizations often do not. Indeed, the rapid rise of new apps and wearable health care tracking technology — often in the form of startups without the resources to necessarily prioritize the security of their systems — has greatly increased the potential for data breaches. Notably, that report highlighted several "imperatives" which are now playing out through regulatory and legislative initiatives:

- Define and streamline leadership, governance, and expectations for health care industry cybersecurity;
- Increase the security and resilience of medical device and health IT;
- Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities;
- Increase health care industry readiness through improved cybersecurity awareness and education;
- Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure;
- Improve information sharing of industry threats, risks and mitigations.

Prudent health care organizations will take seriously these imperatives and the need to implement a proactive, risk-based approach to data privacy and cybersecurity within the industry.

So what should companies do?

Privacy By Design/Security By Design

Many companies are catching on to the need for privacy-by-design and security-by-design, which means incorporating data privacy and cybersecurity into the very framework of the product from its inception, rather than as an afterthought. Although getting to market quickly is obviously important, it will be difficult to be commercially successful with a product that is, for example, easily susceptible to DDoS attacks or has critical vulnerabilities that cannot be rapidly patched. Having good cybersecurity and data privacy controls requires conducting a thorough risk assessment of the threats and vulnerabilities to data and systems — a HIPAA requirement that OCR frequently emphasizes — as well as engaging in a continual identification of hazards, evaluating and controlling for risks, and monitoring the effectiveness of such controls over time.

Vendor Management

Given that the security of health tech is only as good as the weakest link in the "connected" chain, companies should take another look at contracts with third-party vendors that may impact device or data privacy or cybersecurity. For example, there are numerous cases where third-party vendors are the source of a data breach, yet the public and regulators still often focus on whether the upstream data owner or manufacturer did enough to prevent the issue. This could be through more aggressive oversight, conducting audits, ensuring appropriate contract language, training or other steps.

Develop a Plan

It is critical for companies to be prepared in advance for privacy and cybersecurity incidents. Having a robust, well-tested and comprehensive incident response plan — practiced through routine tabletop exercises — will go a long way to preparing a company for such an event.

Training

Companies need to ensure their workforces are sufficiently trained in this area. A company can have the best technical security in the world, but that may not be enough to stop an employee from inadvertently giving out access credentials in response to a targeted phishing attack. Companies should train their employees about these and other potential threats — and continue to train them.

This article first appeared in the May 22, 2018, edition of Law360. To learn more about Law360 and Portfolio Media, visit www.law360.com.

Contact

Elliot Golding
Partner, Washington DC
T + 1 202 457 6407
E elliot.golding@squirepb.com