ROPES & GRAY ALERT

Government Enforcement ▪ Health Care

June 14, 2017

Enforcement Considerations for the Health Care Industry in the Wake of the WannaCry Ransomware Attack

Attorneys
Deborah L. Gersh
Laura G. Hoey
David T. Cohen
Andrew O'Connor
Jennifer L. Romig
Megan McFadden

On May 12, 2017, the WannaCry ransomware cryptoworm attacked over 230,000 computers in over 150 countries, holding data on the computers for ransom. WannaCry spread rapidly through networked systems that had not been updated with Microsoft security patches. The attack was particularly alarming because WannaCry victims included a number of hospitals and health systems. The ransomware affected the ability of many hospitals to access patient medical records, billing records, and even data from certain medical devices linked to the hospitals' systems, in some cases interfering directly with hospitals' ability to provide patient care.

In the wake of the WannaCry attack, many organizations have asked themselves what steps they can take to guard against a future attack—and what might happen if they fail to do so. In the first part of this series,[1] our colleagues addressed what Boards of Directors and senior management should ask of their companyies information security and business teams in order to assess how prepared a company is to respond to and recover from a ransomware attack. In this second part of the series, we discuss potential legal ramifications that may result if organizations—especially those in the health care sector—fail to prepare for a ransomware attack. Health care companies face increasingly high expectations around data security and, as the real-world effects of cyber-attacks continue to rise, government authorities may very well take increasingly aggressive steps to ensure companies are taking concerted action to keep patient information safe.

HIPAA Compliance

In the U.S., health care providers such as hospitals (known as "covered entities") must comply with the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act and implementing regulations (collectively, "HIPAA"). HIPAA requires that covered entities and organizations that assist covered entities with certain tasks involving the use or disclosure of patient information (known as "business associates") adopt administrative, physical and technological safeguards to ensure the confidentiality, integrity and availability of patient health information known as "protected health information" or "PHI." Relevant to ransomware attacks, mandatory safeguards include requirements to "allow access [to PHI] only to those persons or software programs that have been granted access rights,"[2] to "protect electronic protected health information from improper alteration or destruction,"[3] and to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[4]

[1] Ropes & Gray, "Don't WannaCry: Ten Questions Boards and Company Management Can Ask in the Wake of Recent Ransomware Attacks," available at:https://www.ropesgray.com/newsroom/alerts/2017/05/Dont-WannaCry-Ten-Questions-Boards-and-Company-Management-Can-Ask-in-the-Wake.aspx.
[2] 45 CFR § 164.312(a)(1).
[3] 45 CFR § 164.312(c)(1).
[4] 45 CFR § 164.312(e)(1).

Federal HIPAA Enforcement—Office for Civil Rights and Department of Justice

Organizations that fail to implement these mandatory safeguards in a satisfactory manner may face liability under HIPAA. The Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") is responsible for enforcing HIPAA. Covered entities and business associates that experience a "breach" of PHI (*i.e.*, an event that compromises the privacy or security of patient information) must affirmatively report such breach to OCR and affected individuals. If there are fewer than 500 individuals affected, OCR may choose to investigate the breach; if there are more than 500 individuals affected, OCR must investigate the breach. Such investigations frequently include an examination of both the factors that may have caused the breach and the covered entity or business associate's general HIPAA compliance. OCR may review an organization's HIPAA compliance for the past six years as part of its investigation. If a covered entity or business associate is found to have violated HIPAA, OCR may impose civil monetary penalties that range from $100 to $50,000 per violation (with an annual maximum fine per violation of $1.5 million), with aggregate penalties trending higher in recent years.

For entities affected by WannaCry or other ransomware attacks, OCR has issued sub-regulatory guidance[5] that indicates a ransomware attack is presumed to be a HIPAA breach unless the organization can make a fact-specific determination that there is a low probability the patient information was compromised by the attack. As we have previously explained,[6] in the eyes of OCR, it may be difficult to conclude that a ransomware attack was not a breach, particularly if there is a "high risk" that the data's integrity was compromised.

In addition, the Department of Justice ("DOJ") has authority to enforce criminal HIPAA provisions prohibiting knowing disclosures of protected data. Over the last ten years, the DOJ has shown increased willingness to pursue criminal penalties for HIPAA violations.[7] In 2015, for instance, four employees of pharmaceutical company Warner Chilcott were convicted of criminal HIPAA violations for reviewing patient records during visits to physicians' offices. HIPAA's criminal provisions would be directly applicable to ransomware attackers; however, enterprising prosecutors could argue that egregious conduct on the part of health care organizations–such as willful blindness to the need for data security measures–amounts to a "knowing" disclosure of patient information and warrants enforcement action. While prosecutors would face an uphill battle charging a ransomware victim with "knowing" complicity in an attack, a breach resulting in significant patient harm may trigger a correspondingly aggressive response from enforcers.[8]

State Attorneys General

State Attorneys General also have authority under federal and often state law to seek damages on behalf of state residents in the event of a health care-related data breach. The HITECH Act of 2009 gave State Attorneys General the power to seek injunction or damages in any instance in which he or she has "reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by" exposure of PHI in violation of HIPAA.[9]

---

[5] HHS, "FACT SHEET: Ransomware and HIPAA," available at: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
[6] Law360, "Inside The HHS Guidance On Ransomware," available at: https://www.law360.com/articles/823234/inside-the-hhs-guidance-on-ransomware.
[7] *See, e.g.*, https://archives.fbi.gov/archives/littlerock/press-releases/2009/lr102609.htm (Arkansas health care workers pleaded guilty to misdemeanor HIPAA violations for accessing patient medical records out of "curiosity."); https://www.justice.gov/archive/usao/are/news/2008/April/SmithLPNplea%20HIPAA%20041508.pdf (Arkansas nurse pleaded guilty to a felony HIPAA violation for sharing health information with her husband for use against a patient in a legal proceeding).
[8] *Bryan v. United States*, 524 U.S. 184, 193 (1998).
[9] 42 U.S. Code § 1320d–5.

In addition to HIPAA, State Attorneys General often have a variety of state law remedies at their disposal to seek redress for patients harmed by a data breach at a hospital or other healthcare provider. Consumer protection statutes, for instance, may provide a cause of action where a data breach was occasioned by an unfair or deceptive act by the healthcare provider,[10] and State Attorneys General may contend that failure to implement appropriate safeguards or a violation of existing policies intended to protect patient information constitutes an unfair or deceptive act. These consumer protection statutes can greatly increase a healthcare company's exposure in the event of a data breach.[11] Many states also have their own data security[12] or health records laws[13] that may provide additional sources of enforcement authority.

The Massachusetts Attorney General's office has been particularly aggressive in exercising its HIPAA authority and pursuing state remedies when patient data is disclosed. Since 2012, Massachusetts has secured settlements in five suits resulting from data breaches at hospitals and other healthcare providers. For example, the Massachusetts Attorney General reached a $750,000 settlement with a community hospital for alleged failure to appropriately protect patient information when backup tapes containing names, Social Security numbers, and medical diagnoses for over 800,000 patients were lost during shipment to an offsite vendor. Later, medical billing company Goldthwait Associates and four pathology groups that used its services paid a total of $140,000 in settlements to the Massachusetts Attorney General when Goldthwait allegedly disposed of patient medical records in a public dump. Even though the pathology groups that contracted with Goldthwait had no active involvement in the allegedly improper disposal of patient information, they were accused of failing to appropriately vet Goldthwait as a service provider.[14] Finally, the Massachusetts Attorney General settled three separate suits against Massachusetts hospitals allegedly arising out of thefts of unencrypted laptops and backup tapes containing patient information. These cases underscore the importance ensuring appropriate protection for patient information—both from inadvertent disclosure and intentional attacks—even after it leaves the healthcare provider's control or premises.

Other State Attorneys General, including those in New York and New Jersey, have shown a willingness to pursue actions under HIPAA. In 2015, New York's Attorney General sought penalties against the University of Rochester Medical Center ("URMC") under HIPAA where a nurse accessed URMC patient records and provided a list of patient names and addresses to a future employer.[15] In addition, the New Jersey Attorney General recently reached a $1.1 million settlement agreement with Blue Cross/Blue Shield after the theft of unencrypted laptops compromised data from nearly 690,000 customers.[16] The complaint alleged broad scale failure to implement appropriate technological controls to protect PHI and PI and failure to train and supervise employees with access to HIPAA-protected information. As data breaches become more common, health care companies should expect more State Attorneys General to embrace the HIPAA enforcement authority granted by the HITECH Act to pursue remedies where state residents are impacted.

Federal Trade Commission

The Federal Trade Commission ("FTC") has authority to bring enforcement actions against certain parties engaged in unfair or deceptive trade practices under Section 5 of the FTC Act.[17] The agency has taken the position that data

[10] *See, e.g.*, M.G.L. c. 93A (Massachusetts Consumer Protection Act).
[11] *See*, Star Tribune, "Accretive is banned from Minnesota," available at: http://www.startribune.com/accretive-banned-from-minnesota-for-at-least-2-years-to-pay-2-5m/164313776/.
[12] *See, e.g.*, M.G.L. c. 93H (Massachusetts Data Privacy Law, imposing a duty to report promptly any known or suspected data breaches and establishing the authority of the Massachusetts consumer affairs bureau to promulgate regulations regarding appropriate data security precautions for businesses).
[13] *See, e.g.*, MINN. STAT. 144.291-.298 (2016) (Minnesota Health Records Act).
[14] *See*, http://www.mass.gov/ago/news-and-updates/press-releases/2013/140k-settlement-over-medical-info-disposed-of-at-dump.html.
[15] *See*, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-university-rochester-prevent-future-patient.
[16] *See*, http://nj.gov/oag/newsreleases17/pr20170217a.html.
[17] 15 U.S.C. § 45.

security failures can constitute unfair or deceptive practices under the statute, and has taken numerous enforcement actions based on that position.[18] Recently, the FTC has increasingly focused these actions against healthcare companies, despite the fact that their data security practices are already regulated by OCR and State Attorneys General.[19] The FTC has also focused on ransomware in the past year, providing a workshop series as well as advice to consumers and businesses on how to avoid and respond to ransomware.[20] The increasing scope of the FTC's enforcement activities, as well as its recent focus on ransomware, should emphasize to healthcare organizations that enforcement in the wake of a ransomware incident may come from a number of regulatory agencies, including the FTC.

The WannaCry attack should be a wake-up call to health care organizations. This month, HHS's Health Care Industry Cybersecurity Task Force categorized health care cybersecurity as "in critical condition" and warned that the industry that health care companies must take "immediate and aggressive" action to secure IT networks and valuable patient data.[21] Increased enforcement activity, high penalties for noncompliance, increasingly sophisticated hacking and ransomware attacks and warnings from Federal agencies have created a perfect enforcement storm for unprepared organizations in the health care industry.

[18] https://www.ftc.gov/enforcement/cases-proceedings/terms/249.
[19] *See, e.g.*, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.
[20] *See* "Ransomware – A closer look," available at: https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look; and "FTC Offers Advice on How to Avoid and Respond to Ransomware Attacks," available at: https://www.ftc.gov/news-events/press-releases/2016/11/ftc-offers-advice-how-avoid-respond-ransomware-attacks.
[21] *See* Health Care Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Health Care Industry," available at: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.