OCR's 2016 Ransomware "Guidance": A Health Care Provider's New Best Friend?

Jeff C.D. Brecht
Lane Powell PC
Portland, OR

Background on Ransomware Attacks

Doomsday-esque ransomware scenarios are having an increasing impact on the health care industry, becoming commonplace in 2016.[1] Security experts and the media have reported that health care providers[2] who have experienced ransomware "attacks" this year have suffered a host of unwelcome challenges.[3] These include preventing staff use of email and other forms of electronic communication, blocking access to large databases[4] (requiring a reverting to antiquated paper charts5), turning away patients or diverting them to other providers,[6] and even experiencing medical machinery disruption.[7] It has also become common knowledge that ransomware "infection vectors" often include malicious emails that frequently are sent by networks ("botnets") of unsuspecting, infected computers.[8] Ransomware infection then occurs when an unwary email recipient either opens a malicious attachment ("Your missed FedEx Delivery Information is Included Confidentially in the Securely Attached Document") or clicks an internet link ("You Won't Believe What the Kittens in this Video Do!!").[9] It's hard to remain at alert when reports of a ransomware apocalypse seem as ubiquitous as the blaring car security alarms that, over time, have become largely ignored.[10] Nonetheless, health care providers understand that to provide appropriate health care[11] and comply with the Health Insurance Portability and Accountability Act's (HIPAA's) Privacy[12] and Security Rules,[13] they must remain constantly vigilant and clearly proactive to keep up with evolving ransomware[14] and other so-called "cyber threats."[15]

OCR's Ransomware "Guidance"

In mid-2016, in response to the increasing uptick in cyber-attacks on health care providers, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released new (and, some might argue, troubling) HIPAA guidance[16] on ransomware. The guidance came in the form of an eight-page "Fact Sheet," made available on HHS' website.[17] Federal and state courts have sometimes cited directly to OCR's online explanations of HIPAA regulations, and OCR's enforcement role with respect to those regulations, in decisions related to HIPAA.[18]

In announcing release of the ransomware guidance, OCR's Director Jocelyn Samuels characterized malicious cyberattacks on electronic health information systems as "[o]ne of the biggest current threats to health information privacy."[19] Ironically, some might consider a statement contained within the Fact Sheet as an additional "threat" to health care providers, given its implications. Six pages into the eight-page Fact Sheet, OCR states: "Unless the covered entity or business associate can demonstrate that there is a…'low probability that the [protected health information] PHI has been compromised,' based on the factors set forth in the Breach Notification Rule, *a breach of PHI is presumed to have occurred*."[20]

Over time, OCR's breach presumption could have substantial repercussions for the health care industry. Ransomware generally is assumed to encrypt data[21] without permitting ransomware cyber criminals to actually access the infected data.[22] For this reason, some persons who have previously analyzed ransomware attacks may have started their analysis with the presumption that a ransomware attack was merely a HIPAA "security incident."[23] Under that approach, one could fairly easily conclude that most ransomware attacks, by their nature, did not acquire, access, use, or disclose PHI, and were not full blown PHI breaches.[24]

Now, under OCR's 2016 guidelines, it appears that providers infected with ransomware must instead start with the presumption that PHI was breached. This means that, where ransomware has historically been considered by many to be a (potentially costly) annoyance to providers,[25] OCR's new automatic HIPAA breach presumption could make ransomware attacks even more costly, from both a financial and a public relations perspective. It is possible that OCR's 2016 HIPAA guidelines could cause providers to conclude that more ransomware attacks are breaches. If so, that means that HIPAA breach notification rules could be triggered.[26] Providers whose ransomware breaches affect 500 or more individuals also would have the unenviable distinction of being included on OCR's notorious "Wall of Shame."[27]

The Fact Sheet does offer some solace, however, in that it explains that the PHI breach presumption is rebuttable. To rebut the breach presumption, providers must show that, notwithstanding the ransomware infection, there is a "low probability" any PHI was compromised. OCR does not define the term "low probability."[28] Instead, pursuant to HIPAA's breach notification rule, to determine whether the probability that PHI was compromised by ransomware is low, providers must conduct a risk assessment based on four factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who accessed the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.[29] By way of example, OCR suggests that even if the ransomware infection "deletes the original data and leaves only the data in encrypted form," if the impact is mitigated (under factor 4) by "robust contingency plans including disaster recovery and data backup plans," then it may be possible to demonstrate a low probability that PHI was compromised. OCR also "encourages" providers to consider other factors, as appropriate, to analyze the risk that PHI was compromised.

The Fact Sheet also contains information and guidance that by now may be familiar to most providers, such as specific early "indicators" that could mean providers have suffered a ransomware attack and suggesting entities infected by ransomware notify either the Federal Bureau of Investigation or a U.S. Secret Service field office.[30] But, again, what should raise the eyebrows of providers is OCR's statement that, as ransomware attacks become more commonplace, OCR's position is that, if a covered entity or business associate suffers a ransomware infection, then any PHI data impacted by that infection is presumed to be a HIPAA data breach.

So what should providers do in response OCR's 2016 HIPAA/Ransomware guidelines? Read them carefully and embrace them is one viable option. The guidelines offer providers the road map of action that OCR expects providers to take to prevent against, prepare for, respond to, and remediate ransomware attacks. Providers who study that road map, respond to it compliantly, and document that response should be in a strong position to handle ransomware and evolving cyber threats effectively. Bad actors will continue to act badly. Ransomware-type attacks will continue to impact health care providers, and PHI will continue to be breached through such attacks. However, by closely adhering to OCR's guidelines (and frequently monitoring those guidelines for revisions in response to new cyber threats), providers who suffer cyberattacks can place themselves in a strong position to demonstrate to affected individuals, the media, and OCR that the providers took the appropriate steps. Such providers will, among other things, regularly review and update their ransomware/malware policies and procedures. By essentially "friending"[31] OCR's guidelines, providers may find OCR more reasonable and ransomware attacks less costly.[32]

Conclusion

Only time will tell whether OCR's presumption will result in a greater number of reported HIPAA breach notifications. Without question, however, the analysis of HIPAA privacy and security issues (and security incidents)[33] can be complex, including whether a ransomware infection creates a "low probability" that PHI was compromised. Providers should confer with legal counsel and other appropriate professionals to assist with HIPAA Security Rule compliance, and how to analyze and plan to prevent, prepare for, and respond to ransomware attacks.

1 Mark Ward, "*Alarming" rise in ransomware tracked*, BBC News (June 7, 2016), *available at* http://www.bbc.com/news/technology-36459022. ("Ransomware samples seen by [Intel Security] had risen by more than a quarter in the first three months of 2016.").

2 For brevity, in this article the term "health care provider" or "provider" refers generally to all Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates, as defined at 42 C.F.R. § 160(4).

3 United States Computer Emergency Readiness Team (US-CERT), *Ransomware and Recent Variants* (rev. Sept. 30, 2016), *available at* https://www.us-cert.gov/ncas/alerts/TA16-091A.

4 Stacy Cowley and Liam Stack, *Los Angeles Hospital Pays Hackers $17,000 After Attack*, N.Y. Times, Feb. 18, 2016, *available at* http://www.nytimes.com/2016/02/19/business/los-angeles-hospital-pays-hackers-17000-after-attack.html?_r=0.

5 Julia Carrie Wong, *Los Angeles hospital returns to faxes and paper charts after cyberattack*, The Guardian, Feb. 16, 2016, *available at* https://www.theguardian.com/us-news/2016/feb/16/los-angeles-hospital-cyberattack-ransomware-data-computers ("A cyberattack has sent doctors and nurses at a large Los Angeles hospital back to the dark ages—or at least back to the pre-electronic health record days of the 1990s."); *see also* John Woodrow Cox, Karen Turner, and Matt Zapotosky, *Virus infects MedStar Health system's computers, forcing an online shutdown*, Wash. Post, Mar. 28, 2016, *available at* https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html.

6 John Woodrow Cox, *MedStar Health turns away patients after likely ransomware cyberattack*, Wash. Post, Mar. 29, 2016, *available at* https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html.

7 Christiaan Beek, *Ransomware: Coming To A Hospital Near You?*, Intel Security Perspectives (Sept. 26, 2016), *available at* http://www.darkreading.com/partner-perspectives/intel/ransomware-coming-to-a-hospital-near-you/a/d-id/1327010.

8 *An ISTR Special Report: Ransomware and Businesses 2016*, Symantec, at 9-13, *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

9 *Id.*

10 Ilana E. Strauss, *The Alarming Truth: Car alarms don't deter criminals, and they're a public nuisance. Why are they still so common?*, The Atlantic, May 16, 2016, *available at* http://www.theatlantic.com/business/archive/2016/05/car-alarms-dont-work-why-so-common/482769/.

11 Naomi Lachance, *Malware Attacks On Hospitals Put Patients At Risk*, NPR, Apr. 1, 2016 ("Hospitals hit by the attack felt the pressure of being without patient information. At a MedStar hospital, a patient was given an antibiotic that, a nurse told the Washington Post, 'should have been stopped eight hours earlier.'"), *available at* http://www.npr.org/sections/alltechconsidered/2016/04/01/472693703/malware-attacks-on-hospitals-put-patients-at-risk.

12 45 C.F.R. pts. 160 and 164 (subpts. A and E).

13 45 C.F.R. pts. 160 and 164 (subpts. A and C).

14 Mollie Halpern, *FBI This Week: Ransomware on the Rise*, Mar. 25, 2016, *available at* https://www.fbi.gov/audio-repository/news-podcasts-thisweek-ransomware-on-the-rise.mp3/view ("The ransomware threat is evolving as cyber criminals target businesses, local governments, and other organizations.").

15 FBI Director James B. Comey, (Transcript), *The FBI's Approach to the Cyber Threat*, Symantec Government Symposium, Washington, DC (Aug. 30, 2016), *available at* https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat ("the purveyors of ransomware, which is spreading, from our optic, like a virus all across this country and all across the world. Where, for people running a business, it becomes a challenge between choosing paying to get on with your business, or resisting the spread of that virus and helping us fight it and root it out.").

16 OCR is charged with enforcing the HIPAA Privacy Rule, and the Privacy Rule preempts any contrary state law that relates to the privacy of individually identifiable health information that is not "more stringent." 45 C.F.R. § 160.203(b).

17 OCR, Fact Sheet, Ransomware and HIPAA (July 11, 2016), *available at* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

18 *See, e.g.*, *Taylor v. Sherman*, 2014 U.S. Dist. LEXIS 39723 (S.D. Ala. Feb. 24, 2014) (citing to OCR's online explanation that it "is responsible for enforcing the Privacy and Security Rules" of HIPAA); *Cohan v. Ayabe*, 132 Haw. 408, 417 (Haw. 2014) (citing to OCR's online "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the…[HIPAA] Privacy Rule").

19 Jocelyn Samuels, *Your Money or Your PHI: New Guidance on Ransomware* (July 11, 2016), *available at* http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html.

20 Emphasis added.

21 United States Computer Emergency Readiness Team (US-CERT), *Ransomware* (July 11, 2016), *available at* https://www.us-cert.gov/security-publications/Ransomware.

22 This variety of malware is sometimes called "crypto-ransomware." Lucian Constantin, *The number of corporate users hit by crypto ransomware is skyrocketing: File-encrypting ransomware programs are on the rise and companies are increasingly their targets*, PCWorld, July 23, 2016, *available at* http://www.pcworld.com/article/3088076/the-number-of-corporate-users-hit-by-crypto-ransomware-is-skyrocketing.html.

23 The HIPAA term "security incident" means "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 C.F.R. § 164.304 (emphasis added).

24 The HIPAA term "breach" means "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information." 45 C.F.R. § 164.402.

25 OCR, OCR Cyber-Awareness Monthly Update (Mar. 30, 2016), *available at* https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue3.pdf ("Recent cyberattacks on major health care entities have been eye-opening for some healthcare professionals and have changed many views on security for the healthcare sector.").

26 Under HIPAA's rules, breach notification must be provided to affected individuals, HHS, and, if more than 500 individuals are affected, the media. 45 C.F.R. § 164.404-410.

27 OCR, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. OCR's Breach Portal Internet site allows users to search and sort the posted breaches by covered entity name, state, entity type, number of individuals affected, breach date, breach type, and location of breached information (i.e., "Network Server"); *see also* Erica Teichart, *Advocate Health to pay largest HIPAA settlement ever*, Crain's Chicago Business, Aug. 4, 2016, *available at* http://www.chicagobusiness.com/article/20160804/NEWS03/160809896/advocate-health-to-pay-largest-hipaa-settlement-ever (unencrypted laptops containing approximately 4 million patient records were stolen and was the second-largest medical records breach since OCR started publicly posting large incidents to its "wall of shame.").

28 The author has found no case that defines the term "low probability," in the context of HIPAA or otherwise. In the non-HIPAA context of analyzing whether evidentiary error is harmless, some courts have concluded that "high probability" means the court has a "sure conviction" that the error did not prejudice the party against whom the evidentiary error was made. *See, e.g.*, *United States v. Casseus*, 282 F.3d 253, 256 (3d Cir. 2002) (internal quotation marks omitted). It is not clear whether a court, or OCR, might construe "low probability" in the context of HIPAA to mean a "sure conviction" there was no compromise of PHI.

29 45 C.F.R. § 164.402(2).

30 The U.S. Secret Service's website allows users to quickly "Find a Field Office" by simply entering city or zip code into a search field and hitting "GO," *see* http://www.secretservice.gov/contact/field-offices/.

31 In fact, HHS has its own Facebook page, ready for "friending," and HHS regularly posts on HIPAA issues, *see* https://www.facebook.com/HHS/.

32 45 C.F.R. Part 160, Subpart D – Imposition of Civil Money Penalties.

33 45 C.F.R. § 164.304.