Health Law Daily Wrap Up, HEALTH CARE COMPLIANCE NEWS—Global ransomware cyberattack a warning, opportunity for U.S. health providers, (May 17, 2017)

Health Law Daily Wrap Up

Click to open document in a browser

By Kathryn S. Beard, J.D.

A global cyberattack affecting more than 300,000 computers in 150 countries with ransomware known as "WannaCry" led to patient diversion and delay of nonemergency surgeries at hospitals and other health care providers across the United Kingdom's National Health Service (NHS). WannaCry exploits a Microsoft® Windows™ vulnerability; although the software company released a patch to fix that vulnerability in March 2017, many providers and individuals failed to install the patch. At the NHS hospitals, key systems including patient records, diagnostic tests, and telephones were affected beginning on May 12, 2017; four days later, two hospitals continued to divert certain patients. Alisa Chestler, a shareholder with Baker Donelson warned that no provider, even one who has not experienced any cyber disruptions to date, can ignore the WannaCry attack.

WannaCry ransomware. The WannaCry malware is often delivered via emails that trick the user into opening attachments; once downloaded onto a computer, WannaCry locks up computer files and encrypts them to prevent access. It then demands a ransom payment, generally about $300, to release the data back to its owner. The Federal Bureau of Investigation (FBI) does not support paying a ransom in response to a ransomware attack because there is a no guarantee that data will be returned, and such payments may create an incentive for other criminals to attempt similar attacks. The FBI recommends taking precautionary measures to prevent ransomware attacks, and anyone who suspects such an attack should contact the FBI's 24-hour CyberWatch hotline by calling (855) 292-3937 or emailing CyWatch@ic.fbi.gov.

Tips. Chestler offered the following tips to health care professionals to prepare for a similar attack:

- **Communicate.** Prepare and send an alert for employees and staff regarding their roles in preventing such attacks on your networks. Chestler noted that very few emails contain an "emergency"; therefore, everyone should be thoughtful when opening email attachments, even if an email appears to be from a known source. Ensure that all employees know how to access an information technology (IT) help desk 24 hours a day, 7 days a week, because "system incidents are not limited to a 9-5 workday."
- **Review Incident Response Plan.** Ensure communication lines between management, counsel, and key IT personnel are open and ready to implement the incident response plan. The response plan should specifically anticipate a ransomware attack; if not, it should be updated accordingly.Chestler says that documented Incident Response Plans are an expected compliance obligation for all organizations regardless of the size, industry, or kind of information maintained by the systems.
- **Know The Patching Compliance.** Patch Management programs are the lifeblood of any IT security structure. Thousands of organizations were immune to the WannaCry strain of ransomware because they were up-to-date with their patches. Management should ask whether critical patches are up to date, and if not, initiate a plan to get programs as current as possible.
- **Use this As an Opportunity.** Chestler warned that management, legal, and IT security can no longer keep "kicking the can" when it comes to information security. Whether the systems include information on trade secrets or personal information of individuals (including employees) or the systems just keep the machinery up and running, computer systems and programs are the lifeblood of an organization. Chestler says that it is "critical" to know compliance and contractual obligations before an event. She also suggests using this cybersecurity attack as an opportunity to revisit some prior decisions, such as

delays in implementing multi-factor authentication, which Chestler says "is widely becoming the most important information security protocol."

HHS guidance. HHS has resources available to assist providers and suppliers with cybersecurity. A "Dear Colleague" letter released in June 2016 provided information about the threat posed by ransomware (see *Lawmakers, agencies raise specter of ransomware threats to cybersecurity*, June 30, 2016), and the HHS Office of Civil Rights (OCR) soon thereafter published a Fact Sheet on Ransomware and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) (see *With data up for ransom, OCR offers guidance*, August 3, 2016). More recently, CMS sent a letter to state survey agency directors providing reminders and best practices for information security (see *CMS 'HITs' providers in the right direction with cybersecurity resources*, January 18, 2017). Providers should review these resources and then ensure that their own programs, policies, and procedures are up to date to prevent cyberattacks.

Attorneys: Alisa L. Chestler (Baker, Donelson, Bearman, Caldwell & Berkowitz, PC).

IndustryNews: NewsStory ComplianceNews CyberPrivacyFeed FraudNews HITNews HIPAANews