June 19, 2018

Hacking Healthcare

TLP White

We start with a recent survey and simulation finding that threats to medical devices can impact patient safety and then discuss Facebook's request for a federal breach notification law. We also address a HHS's announcement that it will review the effect an upcoming proposed rule will have on small businesses and then shed some light on whether the FDA should consider developing a benchmark for determining if a vendor qualifies for the agency's proposed fast-path program for premarket "software as medical device" approval. We conclude with addressing a survey that found secure messaging has become the number one method for exchanging healthcare data. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Medical Device Threats and Patient Safety.*** The University of California Cyber Team conducted a survey ("survey"), funded by MedCrypt,[1] a medical device data security company, and found that a few healthcare organizations believe between 100 and 1,000 patients have faced adverse health incidents due to healthcare cybersecurity events – e.g., ransomware or malware.[2] Also, a simulation of a hacked medical device scenario conducted by two Doctors found that healthcare professionals may be ill-equipped to handle compromised medical devices.

   The survey asked healthcare organizations to anonymously answer two questions: (1) if respondents were aware of adverse patient incidents resulting from a flaw within one of their devices; and (2) if an attack on their infrastructure resulted in an adverse patient incident. One respondent answered yes to question (1) but did not provide any details and a few respondents answered yes to question (2), noting that the incidents impacted 100 to 1,000 patients. To be fair, the sample size here is small, but results are an important validation of just how real the risk is.

   Dr. Christian Dameff, a researcher and emergency room doctor at UC San Diego, and Dr. Jeffrey Tully, a researcher and pediatrician at UC Davis, conducted a simulation ("simulation") where an actor replicated a situation involving a hacked pacemaker. The

[1] https://www.medcrypt.co/#about

[2] http://www.healthcareitnews.com/news/security-risk-storm-here-medical-device-threats-are-real-and-patient-safety-risk

"patient" presented signs of chest pain and rather than focus on the malfunctioned pacemaker, the participants focused on routine procedures to attempt to save the "patient," which ultimately failed. Doctors Dameff and Tully found that not only were the participants unaware of how to handle the hacked device, they admitted to having no formal training in reacting to a hacked medical device.

2. ***Facebook Responds to Lawmaker Requests Following April Hearings.*** Facebook CEO Mark Zuckerberg provided much anticipated responses to senators' questions following the April hearings on the Cambridge Analytica debacle. In his response to questions about whether Facebook would be receptive to a 72-hour breach notification rule, Mr. Zuckerberg advocated for a federal breach notification law, noting that it would centralize reporting and eliminate some of the existing complexity that makes it difficult to quickly and appropriately protect people in the event of a breach.[3]

   During the April hearing, Senator Lindsey Graham (R-SC) asked whether Facebook would submit proposed regulations for Congress to review. Facebook's response indicated general openness towards regulation and collaborating with regulators to create legislation. However, on the question of actually producing a draft Facebook punted, noting that the social network "would be happy to review any proposed legislation and provide comments."[4] Facebook also reiterated its commitment to protecting people's data and improving security protections, acknowledging that if people don't trust that their information will be safe on Facebook they will not use the service.

3. ***HHS Announcement.*** The US Department of Health and Human Services ("HHS" or "Department") recently announced in the Federal Register,[5] as part of the Department's semiannual regulatory agenda required by the *Regulatory Flexibility Act of 1980*[6] (RFA), that it will examine a proposed rule's impact on small businesses. The rulemaking comes as a result of the *21st Century Cures Act of 2016* ("Cures Act"),[7] which hopes to promote medical product development and innovation.

   The RFA requires federal agencies to assess whether a federal rule burdens small businesses and to determine if regulatory options exist to reduce any burdens posed by the rule. HHS's proposed rule would, among other things (1) implement certain provisions of the Cures Act; (2) include condition and maintenance certification requirements; and (3) create a voluntary nationwide data-exchange network, which would include cybersecurity requirements. There is a possibility that the rule –

[3] https://insidecybersecurity.com/daily-news/facebook-calls-federal-breach-notification-law-response-lawmakers
[4] https://insidecybersecurity.com/daily-news/facebook-calls-federal-breach-notification-law-response-lawmakers
[5] https://www.federalregister.gov/documents/2018/06/11/2018-11239/regulatory-agenda
[6] https://www.sba.gov/advocacy/regulatory-flexibility-act
[7] https://www.fda.gov/RegulatoryInformation/LawsEnforcedbyFDA/SignificantAmendmentstotheFDCAct/21stCenturyCuresAct/default.htm

especially the adoption of a nationwide data-exchange network – may burden small businesses.

The rulemaking, according to HHS, would also "modify the [Office of the National Coordinator for Health IT Certification Program]…to advance health IT certification and interoperability," which according to federal health IT officials, is "a significant step towards achieving interoperability" as laid out by the Cures Act.[8]

4. ***Existing Standards & New Applications: SaMD Precertification.*** The Food and Drug Administration ("FDA") proposal for fast tracking software products through the regulatory approval process has left some wondering how the agency will assess vendor cybersecurity.[9] The proposed software as a medical device ("SaMD") product precertification program is premised on the idea that current regulation of medical device hardware "is not well suited for the faster, iterative design, development and type of validation used for SaMD." The proposal seeks to establish a voluntary program that would allow precertification of cybersecurity vendors of certain medical device software, including mobile apps, which are "intended to treat, diagnose, cure, mitigate or prevent disease or other conditions."

   According to the FDA's working model, a vendor's precertification will depend on an organization-based approach, requiring demonstration of the vendor's "organizational excellence."[10] To evaluate organizational excellence, the FDA will consider five culture of quality and organization excellence principles: (1) product quality; (2) patient safety; (3) clinical responsibility; (4) cybersecurity responsibility; and (5) proactive culture.

   The FDA's plan to fast track SaMD products would make room for medical device innovation by removing some of the regulatory hurdles that have slowed it down. As the commenters pointed out, the FDA does not need to reinvent the wheel here. Existing cybersecurity frameworks and certifications should be the FDA's primary resource in evaluating SaMD products to ensure that innovation and robust cybersecurity develop in tandem.

5. ***Exchanging Health Data Over Secure Messaging.*** Black Book Market Research, a technology and services market research company,[11] conducted a survey of 770 hospital professionals and 1,279 physician practices and found that secure messaging has become the first choice for exchanging health information.[12]

[8] https://www.healthcare-informatics.com/article/interoperability/hhs-releases-draft-trusted-exchange-framework-eyes-creating-network

[9] https://www.healthcareinfosecurity.com/should-fda-create-cybersecurity-measuring-stick-a-11074

[10] https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/UCM605685.pdf

[11] https://blackbookmarketresearch.com/about-us

[12] https://healthitsecurity.com/news/secure-texting-becoming-1st-choice-for-sending-healthcare-data

> Specifically, the survey found that 85 percent of hospitals and 83 percent of physician practices are relying on secure communication services like Doc Halo, PerfectServe, Patient Safe Solutions, Vocera, and Imprivata, to communicate with care teams, patients, and families. Ninety-six percent of hospitals also reported they are budgeting and/or investing in comprehensive clinical communication systems in 2018 and 90 percent of hospital leaders and 94 percent of physicians reported that mobile technology in the healthcare industry is improving patient safety and outcomes.
>
> The survey, however, also found that 30 percent of respondents reported that they still receive daily unsecured communication – which includes personal identifiable information such as birthdays, initials, or partial to full names – and that the two biggest obstacles for using secure messaging is physician buy-in (54 percent) and sufficient funding (48 percent).
>
> The survey shows that the trend for secure messaging is only growing and becoming more and more popular among healthcare professionals and their patients.

Congress –

Tuesday, June 19:
--Hearing to examine Cambridge Analytica and other Facebook partners, focusing on data privacy risks (Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security)[13]
--Hearing to examine changing the trajectory of Alzheimer's, focusing on reducing risk, detecting early symptoms, and improving data (Senate Committee on Aging)[14]

Wednesday, June 20:
--No relevant hearings

Thursday, June 21:
--No relevant hearings

Conferences and Webinars –

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>

[13] https://www.senate.gov/committees/committee_hearings.htm
[14] https://www.senate.gov/committees/committee_hearings.htm

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>

--NH-ISAC Blended Threats Exercise Series – MN (7/25) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>

--NH-ISAC Blended Threats Exercise Series – CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>

--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>

--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>

--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Dems question FCC's claim of cyberattack during net neutrality comment period** <http://thehill.com/policy/technology/391813-dems-question-fccs-claim-of-cyberattack-during-net-neutrality-comment>

-- **Can Verizon Build a Strong Brand From the Bones of Yahoo and AOL?** <https://www.wired.com/story/can-verizon-build-a-strong-brand-from-the-bones-of-yahoo-and-aol>

-- **Sizing up Chinese, North Korean cyberattacks** <https://www.politico.com/newsletters/morning-cybersecurity/2018/06/15/sizing-up-chinese-north-korean-cyberattacks-252481>

-- **Decades-old PGP bug allowed hackers to spoof just about anyone’s signature** <https://arstechnica.com/information-technology/2018/06/decades-old-pgp-bug-allowed-hackers-to-spoof-just-about-anyones-signature/>

-- **Going to the World Cup? Leave the Laptop at Home** <https://www.wired.com/story/world-cup-2018-travel-russia-secure-devices>

-- **Cyber attack on Mexico campaign site triggers election nerves** <https://www.reuters.com/article/us-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerves-idUSKBN1J93BU>

-- **Police Use of Minority Report-Style Pre-Crime Tech Raises Inaccuracy Concerns**

June 19, 2018

<https://www.bleepingcomputer.com/news/government/police-use-of-minority-report-style-pre-crime-tech-raises-inaccuracy-concerns/>
-- **Forcepoint execs: CrowdStrike's warranty is nothing more than marketing**
<https://www.cyberscoop.com/forcepoint-crowdstrike-warranty-marketing-gimmick/>
-- **Hackers mined $90,000 worth of Monero with a simple Docker Hub trick**
<https://www.cyberscoop.com/hackers-mined-90000-worth-monero-simple-docker-hub-trick/>
-- **Despite AI ethical concerns, IoT and smart sensor investments on rise new report finds**
< http://www.healthcareitnews.com/news/despite-ai-ethical-concerns-iot-and-smart-sensor-investments-rise-new-report-finds >

Contact us: follow @NHISAC and email at contact@nhisac.org