June 26, 2018

TLP White

We start by continuing our discussion from last week regarding the FDA's precertification plans. We also address next generation medical devices and IoT areas and then shed some light on a new Apple macOS discovery. We conclude with addressing a recent judgement requiring a cancer hospital to pay $4.3 million as a result of an incurring three data breaches. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Update Released for FDA Pre-Certification Program.*** Last week we reported on the Food and Drug Administration's ("FDA") Software as a Medical Device ("SaMD") pre-certification program, intended to accelerate the regulatory approval process for medical device software and applications. This week, the FDA released an update to its working model for the program.[1]

   As a reminder, the FDA's stated intent here is to recognize that software is different than hardware in that it tends to be updated frequently, which means reviewing the software itself can be unviable. The problem is only growing as software and more complex medical devices that rely on software continue to proliferate. As a result, they propose reviewing the actual software developers, the thought being that as developers prove themselves to be trustworthy, there is increased likelihood that their products will be as well.

   In response to concerns that the model would favor more well-established firms, the updated version clarifies that pre-certification is available to small companies and startups, not just large, established technology companies.[2] It also explains that the FDA's long term plan is to permit pre-certification for both software as a medical device as well as software within a device. Additionally, the updated version incorporates concepts from the International Medical Device Regulators Forum's ("IMDRF") Software as a Medical Device document. The IMDRF is a voluntary group of medical device

[1] https://www.regulations.gov/document?D=FDA-2017-N-4301-0073
[2] https://www.healthcaredive.com/news/fda-unveils-software-pre-cert-update/526224/

regulators working to accelerate international medical device regulatory harmonization and convergence.[3] Finally, the FDA eliminated the need for a predicate device, which qualifies a product for the 510(k) clearance process.[4]

2. ***Next Generation Medical Devices and IoT Areas.*** As we've discussed several times in the past, the healthcare industry is utilizing technology like medical devices, IoT, and software to help treat their patients and streamline the healthcare process. *Healthcare IT News* recently ran an interesting piece addressing, among other things, three "next generation" areas that the healthcare industry should keep an eye out for: (1) real-time analysis of device data; (2) sensing; and (3) patient experiences.[5]

   Real-time capture, access, and analysis of data – the first next generation area addressed – can help streamline significant aspects of the healthcare industry and according to Brian Lawrence, chief technology officer at Hill-Rom Welch Allyn, a global medical technology company,[6] "is essential to helping patients get better care." Indeed, according to Lawrence, the average age of data associated with electronic health records ("EHR") is five hours, which is "too old to be of any predictive use for a patient who needs care now." Real time capture alleviates that problem, allowing healthcare providers to monitor, collect, and analyze a patient's information immediately.

   Sensing – the second next generation area discussed – is building on existing technology to improve the healthcare industry. According to Lawrence, by applying a different perspective to existing technology, sensing can be applied to multiple scenarios, offering the healthcare industry a variety of datasets to work with. For example, as discussed in the article, most hospital beds can weigh a patient and alert hospital personnel if a patient exits the bed but with some advanced algorithms, that same sensing technology can collect data associated with the patient's movement and help with the anticipation of a fall or a potential harmful event.

   Patient experience – the third next generation area addressed – hopes to focus on total patient care – i.e., physical and emotional care – that considers patient comfort and control. Lawrence said, "We need to design devices with simple patient controls that are easy to access; devices that are more comfortable and quiet." For example, Lawrence explained the idea of incorporating ergonomic controls and features into a patient's bed to increase comfort and "make patients feel empowered over their environment, less like prisoners and more like VIPs…"

---

[3] http://www.imdrf.org/

[4] https://www.politico.com/newsletters/morning-ehealth/2018/06/20/fda-rolls-out-pre-certification-update-259530

[5] https://www.healthcareitnews.com/news/next-gen-medical-devices-security-ai-rethinking-design-patient-experience

[6] https://www.hill-rom.com/usa/Our-Company/About-us/Company-Overview/

To read the entire piece, which also addresses industry-academic collaboration efforts as well as ways to rethink the design of medical devices, please follow this link: https://www.healthcareitnews.com/news/next-gen-medical-devices-security-ai-rethinking-design-patient-experience.

3. ***Apple macOS QuickLook Flaw.*** Apple macOS security experts Wojciech Reguła and Patrick Wardle recently published blog posts which detail a flaw stemming from cached data from encrypted hard drives.[7] When macOS users navigate to folders on Finder, the macOS search function, Finder automatically loads icons for the files located in the folders. A new feature in Finder called QuickLook allows users to hold down the Space key while selecting a file to view an image-like preview of the document's contents.

   As part of the QuickLook feature, Finder creates and caches thumbnails for images and other files types stored on encrypted hard drives and partitions. The cached thumbnails are then stored on non-encrypted hard drives, and risk retrieval by malware or forensic tools which could reveal content that should have been encrypted.

   As explained in the posts, this flaw has been known for years, and has persisted as a professional secret known by forensics experts. The bloggers hope that the posts will alert users to the QuickLook flaw so that they are able to take preemptive measures, including explaining how users can delete the thumbnail cache and clear compromising thumbnails from non-encrypted sections of their device. Members that would like more details can check out the Regula post[8] as well as the Wardle post. [9]

4. ***OCR Victory Over HIPAA Violation.*** A large healthcare facility is facing $4.3 million in penalties for violating the Health Insurance Portability and Accountability Act ("HIPAA") in connection with three separate data breaches that occurred in 2012 and 2013.[10] The decision marks the Office for Civil Rights' ("OCR") second summary judgment victory in the sub-agency's history of enforcing HIPAA.[11] Additionally, the organization's $4.3 million fine is the fourth largest amount awarded to OCR by an Administrative Law Judge ("ALJ") or secured in a settlement for HIPAA violations.

   The Health and Human Services proceeding resulted from breaches that occurred in 2012 and 2013 involving the theft of an unencrypted laptop belonging to an employee of this organization and the loss of two unencrypted USB flash drives that contained patient information, including electronic protected health information. Steven T. Kessel, the ALJ presiding over the matter, noted that the facility "implemented written

[7] https://www.bleepingcomputer.com/news/apple/macos-breaks-your-opsec-by-caching-data-from-encrypted-hard-drives/
[8] https://wojciechregula.blog/your-encrypted-photos-in-macos-cache/
[9] https://objective-see.com/blog/blog_0x30.html
[10] https://www.law360.com/texas/articles/1054827/texas-cancer-center-owes-4-3m-for-hipaa-failings
[11] https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html

encryption policies and requirements as far back as 2006, but had been lax in the actual implementation of such protocols."[12]

As a result of this large healthcare organization's failure to implement adequate safeguards, electronic protected health information ("ePHI") belonging to more than 33,000 individuals was lost or stolen between the 2012 and 2013 incidents. The ALJ suggested that the fine imposed on this facility could have been higher based on the severity of the infraction. The penalty suggested by OCR and ultimately approved by the ALJ was $2,000 per day from March 24, 2011 to January 25, 2013 for failing to implement technical procedures and safeguards concerning ePHI in addition to a $1.5 million per year fine for improper use or disclosure of protected health information in 2012 and 2013.[13]

The large healthcare organization has stated that they plan to appeal the decision, citing "key exhibits and arguments" that weren't considered during the proceedings.

Congress –

Tuesday, June 26:
--Hearing entitled, "VA Electronic Health Record Modernization: The Beginning of the Beginning" (House Committee on Veterans' Affairs)[14]
--Joint Hearing entitled, "Artificial Intelligence – With Great Power Comes Great Responsibility" (House Subcommittee on Research and Technology; House Subcommittee on Energy)[15]

Wednesday, June 27:
--Hearing to examine how to reduce health care costs, focusing on understanding the cost of health care in America (Senate Committee on Health, Education, Labor, and Pensions)[16]

Thursday, June 28:
--No relevant hearings

Conferences, Webinars, and Summits –

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

[12] https://www.law360.com/texas/articles/1054827/texas-cancer-center-owes-4-3m-for-hipaa-failings
[13] https://www.hhs.gov/sites/default/files/alj-cr5111.pdf
[14] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108428
[15] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108474
[16] https://www.senate.gov/committees/committee_hearings.htm

--NH-ISAC & Boston Scientific Medical Device Security Workshop – Maple Grove, MN (7/24) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-maplegrove-mn/>
--NH-ISAC Blended Threats Exercise Series – MN (7/25) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Basic Best Practices in Cybersecurity – Abilene, TX (7/31) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-texas-2/>
--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/>
--Biotech/Pharma Security Workshop at Amgen – Tokyo, Japan (8/29) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-at-amgen-tokyo/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--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/>
--NH-ISAC & Cleveland Clinic Medical Device Security Workshop – Breachwood, OH (10/17-18) <https://nhisac.org/events/nhisac-events/medical-device-security-workshop-at-cleveland-clinic-beachwood-oh/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Demployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Hackers who sabotaged the Olympic games return for more mischief** <https://arstechnica.com/information-technology/2018/06/hackers-who-sabotaged-the-olympic-games-return-for-more-mischief/>

June 26, 2018

-- **First in MC: New bill seeks to avert future IT risks**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/06/19/first-in-mc-new-bill-seeks-to-avert-future-it-risks-258382>
-- **The Man Who Saw the Dangers of Cambridge Analytica Years Ago**
<https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica>
-- **Maryland woman pleads guilty to using IDs from massive U.S. government hack**
<https://af.reuters.com/article/worldNews/idAFKBN1JF09M>
-- **Rootkit-Based Adware Wreaks Havoc Among Windows 10 Users in the US**
<https://www.bleepingcomputer.com/news/security/rootkit-based-adware-wreaks-havoc-among-windows-10-users-in-the-us/>
-- **Inside the Crypto World's Biggest Scandal**
<https://www.wired.com/story/tezos-blockchain-love-story-horror-story>
-- **Cisco CPO: Privacy Is Not About Secrecy or Compliance**
<https://www.darkreading.com/operations/cisco-cpo-privacy-is-not-about-secrecy-or-compliance/d/d-id/1332082>
-- **Private sector warms to U.S. Cyber Command carrying out 'hack backs'**
<https://www.cyberscoop.com/cyber-command-hack-back/>
-- **Google to Fix Location Data Leak in Google Home, Chromecast**
<https://krebsonsecurity.com/2018/06/google-to-fix-location-data-leak-in-google-home-chromecast/>
-- **Senate Votes to Reimpose ZTE Ban Despite President Trump's Efforts**
<https://www.bleepingcomputer.com/news/government/senate-votes-to-reimpose-zte-ban-despite-president-trumps-efforts/>

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