April 24, 2018

TLP White

We have a lot of exciting topics this week. First, we start with news coming out of the federal agencies. The FDA recently released a new medical device plan which includes cybersecurity and the NIST updated its well-known Cybersecurity Framework. We then focus on the use of hybrid cloud systems and shed some light on Facebook's new attempt at privacy in the wake of Cambridge Analytica. We also address some activity going on at ICANN and conclude with a discussion on a recent state AG settlement regarding a health data privacy breach. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Agency News. FDA Medical Device Plan:*** The U.S. Food and Drug Administration ("FDA") recently released a five-point plan focused on improving medical device safety.[1] According to FDA Commissioner Scott Gottlieb, M.D., "[The FDA's plan] aim is to make sure that the new advances in technology that are enabling better capabilities and benefits are also harnessed to bring added assurances of safety, so that more patients can benefit from new devices and address unmet needs."

   The plan focuses on: (1) creating medical device safety protection in the U.S.; (2) exploring regulatory mechanisms to simplify and improve on implementing postmarket mitigations; (3) promoting innovation; (4) increasing medical device cybersecurity; and (5) consolidating the FDA's Center for Devices and Radiological Health premarket and postmarket offices.

   According to the cybersecurity portion of the plan, the FDA would: (1) compel manufacturers to ensure their medical devices include features that permit software updates and security patches; (2) update its premarket cybersecurity guidance on medical devices to improve risk protection and mitigation; (3) consider requiring manufacturers to disclose vulnerabilities as vulnerabilities are identified; and (4) explore creating a public-private partnership that consists of hardware, software, networking, biomedical engineering, and clinical experts to assist with device vulnerability

[1] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm604672.htm

coordination and response as well as act as a resource for the private sector and the FDA.[2]

The FDA is currently soliciting feedback so for those members who'd like to take advantage of this opportunity, they may submit comments to the FDA through the public docket (FDA-2018-N-1315) at www.regulations.gov.

2. ***Agency News. NIST Updates the Cybersecurity Framework:*** The National Institute for Standards and Technology ("NIST") recently released an update to its Cybersecurity Framework called the Cybersecurity Framework 1.1 ("1.1").[3] According to U.S. Secretary of Commerce Wilbur Ross, 1.1 "should be every company's first line of defense…[and] [a]dopting version 1.1 is a must do for all CEO's."[4]

   Cybersecurity Framework 1.1, like its predecessor, is a voluntary, risk-based approach to cybersecurity and was created through a collaborative effort involving industry, academia, and government to focus on protecting critical infrastructure. Unlike 1.0, however, 1.1 expands the scope of the framework from just the energy, banking, communications, and defense industries to all industry sectors and provides an update to: (1) authentication and identity; (2) self-assessing cybersecurity risk; (3) managing the cybersecurity of the entire supply chain; and (4) vulnerability disclosure.

   Specifically, the Framework consists of three parts: (1) the Framework Core – i.e., "a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors;" (2) Implementation Tiers – i.e., information that "provides context on how an organization views cybersecurity risk and the processes in place to manage that risk;" and (3) a Framework Profile – i.e., a profile that "represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories."[5] Together, these three elements allow users to tailor 1.1 to their specific cybersecurity needs.

   If you are interested (and we think you should be), NIST is hosting a free public webcast explaining 1.1 on April 27, 2018 at 1 PM EST and a conference from November 6-8, 2018 in Baltimore, Maryland.[6]

3. ***Tech News. Using a Hybrid Cloud.*** The San Diego Supercomputer Center at UC San Diego ("Center") was one of the first to use cloud computing in the health industry and

---

[2] https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[4] https://www.commerce.gov/news/blog/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[5] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[6] https://www.commerce.gov/news/blog/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

recently adopted a "hybrid-cloud" to help with its research in cancer and the human immune system.[7]

A hybrid-cloud utilizes an interconnected infrastructure of in-house and third-party computing. In practice, the Center's onsite staff operate the Center's physical, on-premises infrastructure while third-party vendors like AWS and Azure operate the Center's cloud services infrastructure. According to Sandeep Chandra, director of the Center's health cyberinfrastructure, the Center "chose a hybrid cloud approach because [the Center has] a large on-premises footprint that is serving some specific use-cases for [its] customers, but… [also] need[s] to leverage the scalability and automation public cloud platforms offer."

4. ***Tech News. Facebook Updates Privacy Practices.*** As the Cambridge Analytica hysteria begins to die down, Facebook has kept itself occupied, unveiling updated privacy policies and practices in anticipation of the European General Data Protection Regulation's ("GDPR") May 25th effective date. This week, Facebook started asking European users for permission to use their personal data for features including facial recognition and some types of targeted advertising.[8] European users will now be prompted as to whether they would like to see targeted ads based on political, religious and relationship details that they share on their profiles or from data collected by Facebook's external partners. Facebook has indicated that U.S. users can expect to be able to review this information in the coming months.

   Facebook's recent privacy changes have multiple purposes. In addition to working towards compliance with the GDPR, they are also part of Facebook's broad efforts to demonstrate that consumers have full control over their data, as Facebook CEO Mark Zuckerberg emphasized throughout his congressional testimony. Despite these efforts, the changes require Facebook users to go through several steps before Facebook accepts the user's decision not to share their data. Facebook officials acknowledged that it is a multi-step process, and insist that the options are clear to consumers.

   The hearings are over, and new policies are going up, but Facebook's privacy rehab – both for GDPR and PR purposes – will continue for the long haul.

5. ***GDPR. ICANN Controversy Goes Full Throttle.*** The Internet Corporation for Assigned Names and Numbers ("ICANN") can't quite figure out how to meet General Data Protection Regulation ("GDPR") standards while preserving current operations, which has provoked a lot of regulatory turmoil on both sides of the pond.[9] ICANN manages the Domain Name System ("DNS") and runs the WHOIS public database of domain name

[7] http://www.healthcareitnews.com/news/supercomputer-center-shows-security-challenges-operating-healthcare-hybrid-cloud

[8] https://www.wsj.com/articles/facebook-provides-a-preview-of-its-privacy-makeover-1524027600?mod=searchresults&page=2&pos=3

[9] https://www.zdnet.com/article/dns-is-about-to-get-into-a-world-of-trouble-with-gdpr/

owners. Anyone with a web domain must register their domain in the WHOIS database as well as their name, address, email address, and phone number. Under the GDPR, collection of personal information, including the information required as part of the domain registration process, triggers certain requirements to ensure that the data is processed lawfully.

ICANN has long been aware that the WHOIS database presents several privacy challenges,[10] and has known for years that WHOIS would not work with the GDPR. Because it has failed to come up with an adequate GDPR compliance plan, ICANN recently asked the Article 29 Working Group, an EU regulatory body, to give ICANN a one year moratorium on enforcement while it continues to try to figure things out. In a recent response, the Article 29 Working Group announced that it would not give ICANN more time. [11] Subsequently, ICANN stated that without a moratorium on enforcement, WHOIS will become fragmented, and that a fragmented WHOIS would no longer employ a common framework for generic top-level domain registration directory services.[12]

6. ***Breach. Vendor Vetting.*** A New Jersey healthcare provider, Virtua Medical, was recently fined for failing to conduct a thorough analysis of the risk to the confidentiality of patient data sent to its third-party vendor.[13] The New Jersey Attorney General recently announced that it is requiring Virtua to pay roughly $418,000 and to improve data security practices to settle allegations that Virtua failed to properly protect the privacy of more than 1,650 patients whose medical records were viewable on the internet following a server misconfiguration by a private vendor.[14]

   The Virtua breach occurred when the transcription vendor that Virtua hired to transcribe dictations of medical notes, letters, and reports by doctors at several Virtua locations, updated software on a password protected File Transfer Protocol website ("FTP Site") where the transcribe documents were kept. According to the Attorney General, during the update, the vendor accidentally misconfigured the web server, which allowed the FTP Site to be accessed without a password. At this point, anyone who searched Google using terms that happened to be contained within the dictation information (including patient names, doctor names or medical terms) was able to access and download the documents located on the FTP Site. Ultimately, a patient discovered the breach when she stumbled upon portions of her own medical records while conducting a Google search. Yikes. Following this discovery, Virtua launched an internal investigation and notified state and federal law enforcement authorities about the incident.

---

[10] https://whois.icann.org/en/history-whois
[11] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf
[12] https://www.icann.org/news/announcement-2018-04-12-en
[13] http://www.healthcareitnews.com/news/new-jersey-fines-virtua-medical-418000-hipaa-breach
[14] http://nj.gov/oag/newsreleases18/pr20180404b.html

April 24, 2018

Congress –

Tuesday, April 24:
--Hearing to examine mitigating America's cybersecurity risk (Senate Committee on Homeland Security and Governmental Affairs)[15]

Wednesday, April 25:
--Hearing to prepare small businesses for cybersecurity success (Senate Committee on Small Business and Entrepreneurship)[16]

Thursday, April 26:
--No relevant hearings

Conferences and Webinars –

--Security Workshops at Intermountain Health – Park City, UT (4/24) <https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--Medical Device and Pharmaceutical Security Workshop – London <https://nhisac.org/events/nhisac-events/security-workshops-london/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17) <http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--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>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--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/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>

[15] https://www.hsgac.senate.gov/hearings/mitigating-americas-cybersecurity-risk.
[16] https://www.sbc.senate.gov/public/index.cfm/hearings?ID=CFEEC903-892D-4BD9-ADC1-DB473EA4AE7F

April 24, 2018

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

Sundries –

-- **New cyber deterrence bill drops**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/04/18/new-cyber-deterrence-bill-drops-175217>
-- **Intel, Microsoft to use GPU to scan memory for malware**
<https://arstechnica.com/gadgets/2018/04/intel-microsoft-to-use-gpu-to-scan-memory-for-malware/>
-- **Researchers: Malware app infecting thousands of Facebook accounts**
<http://thehill.com/policy/cybersecurity/383964-malware-campaign-infects-thousands-of-facebook-accounts-researchers-say>
--'**Trustjacking' could expose iPhones to attack**
<https://www.wired.com/story/trustjacking-ios-itunes-wi-fi-sync-attack>
-- **Simply and Secure Your Online Logins with Yubikey**
<https://www.wired.com/story/how-to-use-a-yubikey>
--**Welcome to the Wikipedia For Terms of Service Agreements**
<https://www.wired.com/story/terms-of-service-didnt-read>
--**U.S., Britain blame Russia for global cyber attack**
<http://feeds.reuters.com/~r/Reuters/worldNews/~3/m7fEeBMp7Hg/u-s-britain-blame-russia-for-global-cyber-attack-idUSKBN1HN2CK>
-- **Bangladesh eyes settlement in U.S. cyber heist suit ahead of its own case**
<http://feeds.reuters.com/~r/Reuters/worldNews/~3/Wtt1QPFRs_s/bangladesh-eyes-settlement-in-u-s-cyber-heist-suit-ahead-of-its-own-case-idUSKBN1HN1MZ>
-- **48 million profiles left exposed by data scraping firm, report says**
<https://www.cyberscoop.com/localblox-upguard-data-scraping-breach/>
-- **Symantec, Fortinet announce new security tools with analytics, automation for cyber response**
<http://www.healthcareitnews.com/news/symantec-fortinet-announce-new-security-tools-analytics-automation-cyber-response

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