April 3, 2018

Hacking Healthcare

TLP White

We have a lot of news coming out of the U.S. agencies this week. We start first with a recent HHS announcement discussing the importance of creating a contingency plan to recover from cyberattacks and then address a recent FTC announcement urging the use of vendor contracts to reduce cybersecurity risks. We then continue last week's discussion about breach notification legislation. We also provide a brief analysis of TLS 1.3 and conclude with a discussion about a major mobile fitness application breach. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Agencies.* Contingency plan, anyone?** The U.S. Department of Health and Human Services Office for Civil Rights ("OCR"), in its March newsletter,[1] noted that organizations must have a contingency plan in place to respond to a cyberattack.[2] The agency said, "The purpose of any contingency is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event." Specifically, OCR notes that the HIPAA Security Rule requires HIPAA covered entities and business associates to create a contingency plan that includes: (1) a disaster recovery plan to restore protected health data; (2) an emergency mode operation plan to maintain and protect critical security functions; and (3) a data backup plan to regularly copy protected health data to assist with the data restoration process.

   OCR recommends that organizations create a formal policy and establish specific guidelines and procedures for their contingency plan as well as incorporate the plan into normal business operations. That way, organizations can become familiar with the plan before a cyberattack takes place and be prepared for one when it does. Moreover, OCR recommends organizations communicate the plan to its employees and review it regularly to identify vulnerabilities and provide adequate updates.

[1] https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf

[2] https://www.beckershospitalreview.com/cybersecurity/ocr-3-steps-to-create-a-cyberattack-contingency-plan.html

2. ***Agencies.*** **Using Contracts to Address Vendor Risk.** The Federal Trade Commission ("FTC") chief of privacy and identity protection Molly Crawford recommends using contracts and vendor oversight as a mechanism for minimizing the cybersecurity risks associated with handling medical information and personal health records.[3] Ms. Crawford shared this recommendation during last Tuesday's National HIPAA Summit. During the event, she addressed the changing nature and use of personal medical information in the wake of emerging internet-based services and apps that can track physical conditions and activities while also posing increased cybersecurity and identity-theft risks. Ms. Crawford recommends that companies put contracts in place that specifically address privacy and security for protected health information and noted that healthcare providers need to provide "oversight for their service providers" in addition to including specific contractual requirements in the vendor agreements.

Notably, Ms. Crawford mentioned the FTC's ongoing consumer protection efforts, and the agency's increasing role in spaces that could impact healthcare providers as well as health technology developers. She highlighted that sensitive information about an individual's physical conditions such as age, activity level and dietary preferences falls outside of HIPAA and is not regulated by Health and Human Services. Her remarks suggest that we should expect the FTC to be vigilantly monitoring security practices in the healthcare and health technology space.

3. ***State and Federal Breach Notification Legislation.***

The back-and-forth regarding State vs Federal breach notification goes on. As you'll see below, State AGs seem to think they have the problem well in hand, but the complex array of evolving State breach notification laws continue to be a burden for organizations that find themselves required to notify.

Alabama. Continuing from last week's discussion, the Alabama House of Representatives joined the Senate in passing the Data Breach Notification Act ("SB 318"). The bill now awaits the governor's signature.[4] If enacted, the law would (1) require organizations to notify victims of a breach, (2) include medical and health insurance information in its definition of "personally identifying information," and (3) permit the Attorney General's Office to issue fines and file suit on behalf of the victims if organizations failed to issue notifications.[5] If the governor signs off soon, the law would go into effect in the next few months.[6]

[3] https://insidecybersecurity.com/daily-news/ftc-official-urges-use-contracts-address-vendor-risks-ensure-security-health-data

[4] http://alisondb.legislature.state.al.us/alison/SESSBillStatusResult.ASPX?BILL=SB318&WIN_TYPE=BillResult

[5] http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2018RS/PrintFiles/SB318-enr.pdf

[6] https://www.lexology.com/library/detail.aspx?g=3150e601-aba4-47b7-ab4e-4eaa3560aff0

South Dakota. South Dakota beat Alabama to the punch and is officially the 49th state to enact a breach notification law.[7] The law goes into effect on July 1, 2018 and requires any person or business doing business in South Dakota ("information holder") that owns or licenses computerized data from South Dakota residents to comply with the law.

Specifically, the law requires information holders to notify victims and consumer reporting agencies through mail or electronically, no later than 60 days from discovery, if an authorized user acquired or believed to have acquired a victim's personal or protected information.[8] However, an information holder need not make a disclosure if, after conducting an investigation and notifying the Attorney General ("AG"), it "reasonably determines" the breach will not result in harm.[9] Nonetheless, notification to the AG is required if the breach impacts more than 250 South Dakota residents.

Federal. AGs from 31 states and the District of Columbia have written an open letter to the U.S. House of Representatives opposing the Data Acquisition and Technology Accountability and Security Act, a bill that would create federal breach notification requirements.[10] The state AGs argue that the federal law would preempt state law resulting in watered down state laws and only focus on large breaches - i,e., breaches affecting 5,000 or more individuals.

4. ***Latest in Tech.*** **TLS 1.3: coming to a browser near you.** Over four years and 28 drafts later, the Internet Engineering Task Force ("IETF") approved a new industry standard for secure connections, also known as Transport Layer Security ("TLS") version 1.3.[11] The new standard will make all secure internet connections faster because of decreased clutter in computer-to-computer communication. The faster speed will in turn make TLS more secure by eliminating old, obsolete encryption.

   In the last two years of TLS 1.3 development, the financial and banking industries raised concerns that the new standard prevents banks from being able to decrypt and monitor TLS connections. As such, financial industry security professionals requested that TLS 1.3 include a backdoor to allow them to monitor TLS traffic. Ultimately the backdoor was rejected by the IETF because it would eliminate the security advantages created by the new protocol.

5. ***Breach of the Week.*** **MyFitnessPal.** On March 25, 2018, diet, nutrition and exercise tracking app MyFitnessPal, which is owned by Under Armour, experienced a data breach

[7] https://www.lexology.com/library/detail.aspx?g=f4eadca4-97bf-4b00-a217-f722781b43f2
[8] https://www.lexology.com/library/detail.aspx?g=f4eadca4-97bf-4b00-a217-f722781b43f2
[9] http://sdlegislature.gov/docs/legsession/2018/Bills/SB62ENR.pdf
[10] http://www.illinoisattorneygeneral.gov/pressroom/2018_03/Committee_Leaders_letter.pdf
[11] https://www.cyberscoop.com/tls-1-3-approved/

affecting 150 million users.[12] Unfortunately for MyFitnessPal, this event marks the largest breach of 2018, though if history is any guide, they aren't likely to hold on to the dubious honor long. The information involved in the breach was limited to user names, email addresses and hashed passwords.

We'll keep an eye on this as details unfold.

Congress –

Tuesday, April 3:
--No relevant hearings scheduled

Wednesday, April 4:
--No relevant hearings scheduled

Thursday, April 5:
--No relevant hearings scheduled

Conferences and Webinars –

<https://vendome.swoogo.com/2018-Cleveland-Health-IT-Summit>
--Health IT Summit – San Francisco, CA (4/5) <https://vendome.swoogo.com/2018-San-Francisco-HIT-Summit>
--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>

[12] https://threatpost.com/under-armour-reports-massive-breach-of-150-million-myfitnesspal-accounts/130863/

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

Sundries –

--**Hackers disrupt Baltimore's emergency call system; Atlanta still affected** <https://www.reuters.com/article/us-usa-cyber-baltimore/hackers-disrupt-baltimores-emergency-call-system-atlanta-still-affected-idUSKBN1H42I2>
--**Boeing said detected limited intrusion of malware** <https://www.reuters.com/article/us-cyber-boeing/boeing-said-detected-limited-intrusion-of-malware-idUSKBN1H43H3>
--**Internet firms should do 'much more' more to remove illegal content: UK interior minister** <https://www.reuters.com/article/us-britain-security-cyber-rudd/internet-firms-should-do-much-much-more-to-remove-illegal-content-uk-interior-minister-idUSKBN1H418A>
--**Proper Paper Records Disposal Necessary for PHI Data Security** <https://healthitsecurity.com/news/proper-paper-records-disposal-necessary-for-phi-data-security>
--**Threat Intelligence Sharing Essential for Healthcare Cybersecurity** <https://healthitsecurity.com/news/threat-intelligence-sharing-essential-for-healthcare-cybersecurity>
--**Data Security Key Consideration for Healthcare Blockchain Success** <https://healthitsecurity.com/news/data-security-key-consideration-for-healthcare-blockchain-success>
--**Security is for life, not just for Christmas: UK review of the security of consumer IoT products** <https://www.lexology.com/library/detail.aspx?g=048f465d-7412-4a2c-96bc-ca400b11690a>
--**Data security: The bad guys are stepping up their game. Are you?** <https://www.lexology.com/library/detail.aspx?g=dc2122e8-439f-48e3-b81c-480b595f5cdd>
--**New York offers free cyber security tools to public to deter hackers** <https://www.reuters.com/article/us-usa-cyber-new-york/new-york-offers-free-cyber-security-tools-to-public-to-deter-hackers-idUSKBN1H52XC>
--**Government's supply chain risk is drawing more attention than ever, Capitol Hill aides say** <https://www.cyberscoop.com/supply-chain-risk-transparency-know-identity-conference/>

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