



TLP White

We start first with a GDPR update. We then focus on a new healthcare Blockchain alliance program and address a data breach lawsuit filed against CVS and a FinTech company. We conclude with a discussion about a new medical device security startup and a quick update regarding Alabama's Breach Notification Law. Welcome back to *Hacking Healthcare*:

Hot Links –

1. **EU. GDPR.** We checked, and the GDPR deadline of May 25, 2018 keeps getting closer, so no temporal reprieve in sight. As you will recall, over the course of our February issues, we gave a general overview of the GDPR's approach, and primed our members with some key terminology and practical implementation steps. In the spirit of keeping the GDPR top of mind, this week we will highlight a few GDPR to-do items that should be at the top of your list (if not already completed).
 - ✓ **Know what data you have** – be clear on the types of data that your organization holds. Under the GDPR, processing of genetic data, biometric data, and other types of health data require special attention. Outlining the types of data that you have (including HR data) will help ensure that nothing is overlooked.
 - ✓ **Establish a lawful basis for processing** – once you are clear on the types of data that you hold, make sure that there is a lawful basis for processing that information.
 - ✓ **Update your policies** – Update your internal governance policies as well as externally facing policies such as your privacy policy to make sure that they incorporate GDPR requirements.
 - ✓ **Be prepared to respond to data access requests** - establish a process for handling data access requests from data subjects.
 - ✓ **Have a plan** – prepare/update your breach response plan to reflect GDPR requirements. Also take this opportunity to update internal governance procedures and educate your employees to facilitate GDPR compliance.

If you aren't sure, it's not too late to get some help. GDPR is complex and exactly how the EU will enforce it remains unclear. You don't want to be caught off guard.

- 2. Latest in Tech. Blockchain, meet healthcare.** Maintaining provider directories just got a little easier for five healthcare organizations. UnitedHealthcare, Humana, Optum, Quest Diagnostics and MultiPlan are launching a Blockchain pilot program designed to ease the burdens of mandated provider directories.¹

Blockchain technology logs transactions publicly and chronologically, creating a database of a continuously expanding list of ordered “blocks.”² Each block is time-stamped and connected to the block that came before it, and collectively each block forms a Blockchain. The Blockchain creates an indelible record, allowing an entire community to verify its authenticity rather than relying on a single, centralized authority.

Although Blockchain was originally developed as the accounting method for the virtual currency Bitcoin, Blockchain technology has emerged in several other commercial applications. According to a senior engineer at Optum, the alliance of the five healthcare organizations for the Blockchain pilot program is one of the first, if not the first, national Blockchain alliance for healthcare. The five participating organizations will use Blockchain technology to improve the quality of the data that they maintain, and will reduce the administrative costs associated with maintaining healthcare provider demographic data.

Currently, each payer is responsible for obtaining the same provider information, and providers are often overwhelmed by a high volume of similar requests from various plans. Moreover, insurers expend a lot of resources trying to request information from providers during each 90-day cycle. As much as \$2.1 billion is spent annually across the healthcare system to keep all of this information up to date. Now, with their forces combined, the five organizations participating in the pilot program will be able to share curated information, relying on the security of the Blockchain to safeguard the data.

- 3. Legal News.** On March 21, 2018, a class action lawsuit was filed against CVS Health; Caremark LLC, a CVS Health subsidiary; and Fiserv Solutions LLC, a financial technology company,³ in the US District Court for the Southern District of Ohio.⁴

The lawsuit claims that in the summer of 2017, CVS Health exposed 6,000 individual’s PHI and HIV status as a result of mailing out envelopes with “two clear glassine windows.” According to the lawsuit, the “reference to the recipient’s HIV status was plainly visible through the glassine window” because the defendants failed to follow the Ohio Department of Health’s standard practice of sending “all mailings related to HIV-related issues in opaque, non-windowed envelopes.”⁵ The lawsuit also alleges that the

¹ <http://www.healthcareitnews.com/news/optum-unitedhealthcare-humana-others-launch-blockchain-pilot>

² <http://www.healthcareitnews.com/news/how-does-blockchain-actually-work-healthcare>

³ <https://www.fiserv.com/about.aspx>

⁴ <https://healthitsecurity.com/news/federal-lawsuit-filed-following-alleged-cvs-health-data-breach>

⁵ <https://healthitsecurity.com/images/site/attachments/CVS-class-action.pdf>

April 10, 2018

defendants did not notify affected individuals or the US Department of Health and Human Services about the breach despite receiving a letter from plaintiffs' counsel demanding CVS to do so.

- 4. Latest in Tech. Medical Device Security:** Cynerio, a new medical device security startup,⁶ officially launched after announcing multimillion dollar funding rounds with two medical device investment firms, Accelmed⁷ and Elron.^{8 9}

Cynerio's technology focuses on discovery, visibility, and protection. Specifically, according to Cynerio's website, the technology uses a combination of device behavior learning and medical workflow analysis to offer full visibility of the medical device's performance and network activity as well as detect anomalies and stop threats to patient's safety and data.¹⁰

Just as we saw with personal computers and mobile phones, security companies for medical devices are stepping in to fill gaps in insecure designs. This is a good thing, but building security into medical devices from the beginning should remain a focus for manufacturers and will remain a focus for regulators.

- 5. State Breach Notification Legislation. Better late than never?** Alabama has officially become the 50th state to enact a breach notification law.¹¹ The law (1) requires organizations to notify victims of a breach, (2) includes medical and health insurance information in its definition of "personally identifying information," and (3) permits the Attorney General's Office to issue fines and file suit on behalf of the victims if organizations failed to issue notifications.¹² The law goes into effect on May 1, 2018.

Congress –

Tuesday, April 10:

--No relevant hearings scheduled

Wednesday, April 11:

--Hearing to examine critical consumer data privacy issues (Facebook CEO Mark Zuckerberg will be testifying) (House Energy and Commerce Committee)¹³

⁶ <https://www.cynerio.co>

⁷ <http://www.accelmed.com>

⁸ <https://www.elron.com>

⁹ https://www.darkreading.com/risk/medical-device-security-startup-launches/d/d-id/1331444?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

¹⁰ <https://www.cynerio.co>

¹¹ <https://healthitsecurity.com/news/alabama-last-us-state-to-enact-data-breach-notification-law>

¹² <http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2018RS/PrintFiles/SB318-enr.pdf>

¹³ <https://energycommerce.house.gov/news/press-release/ec-announces-facebook-ceo-mark-zuckerberg-will-testify-april-11th/>

April 10, 2018

--Hearing to examine cyber operations today and preparing for 21st century challenges in an information-enabled society (House Committee on Armed Services)¹⁴

--Hearing to review and assess the Department of Defense budget, strategy, policy, and programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019 (House Subcommittee on Emerging Threats and Capabilities)¹⁵

--Hearing to examine combating the opioid crises and improving the ability of Medicare and Medicaid to provide care for patients (House Subcommittee on Health)¹⁶

Thursday, April 12:

--Hearing to examine the challenges facing DHS's Consolidated Headquarters Project (House Subcommittee on Oversight and Management Efficiency)¹⁷

--Hearing to review the Office of Information and Regulatory Affairs (Senate Subcommittee on Regulatory Affairs and Federal Management)¹⁸

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>>

¹⁴ <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108077>

¹⁵ <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108076>

¹⁶ <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108092>

¹⁷ <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108085>

¹⁸ <https://www.hsgac.senate.gov/hearings/reviewing-the-office-of-information-and-regulatory-affairs>

April 10, 2018

--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 –

--Facebook rewrites terms of service amid data scrutiny

< <http://thehill.com/policy/technology/381628-facebook-rewrites-terms-of-service-amid-data-scrutiny>>

--No Injury? No Problem: Mere Risk of Identity Theft Can Establish Standing

<<https://www.lexology.com/library/detail.aspx?g=9f439dfd-f135-4182-abc2-01a0ef7e5074>>

-- Healthcare Pros Worry about Data Security at Other Organizations

< <https://healthitsecurity.com/news/healthcare-pros-worry-about-data-security-at-other-organizations>>

--CareFirst breached again, notifying 6,800 members of phishing attack

<<http://www.healthcareitnews.com/news/carefirst-breached-again-notifying-6800-members-phishing-attack>>

--Sears Holding, Delta Air hit by customer data breach at tech firm

< <https://www.reuters.com/article/us-delta-air-cyber-24-7-ai/sears-holding-delta-air-hit-by-customer-data-breach-at-tech-firm-idUSKCN1HC089>>

--Massachusetts can sue Equifax over data breach, judge rules

<<https://www.reuters.com/article/us-equifax-cyber/massachusetts-can-sue-equifax-over-data-breach-judge-rules-idUSKCN1HB2QQ>>

--With trade war looming, Chinese cyberespionage may return

<<https://www.cyberscoop.com/us-china-trade-war-cyberattacks/>>

--DARPA is looking to avoid another version of Meltdown or Spectre

<<https://www.cyberscoop.com/darpa-contract-meltdown-spectre/>>

--Microsoft rolls out new ransomware protections

<<http://thehill.com/policy/cybersecurity/381799-microsoft-rolls-out-new-ransomware-protections>>

--One-Third of Internal User Accounts Are 'Ghost Users'

<https://www.darkreading.com/operations/identity-and-access-management/one-third-of-internal-user-accounts-are-ghost-users/d/d-id/1331443?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>

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