September 29th, 2020

TLP White

This week, *Hacking Healthcare* begins by exploring what to expect from the recent announcement by the U.S. Food and Drug Administration (FDA) that the agency has formally launched its Digital Health Center of Excellence. Next, we make note of an update to Health and Human Services' (HHS) freely available Security Risk Assessment tool and why it may be a good place to start for any HIPAA covered entity looking to facilitate compliance with the Security Rule. Finally, we highlight a recent global study that shows just how serious third-party risk can be for organizations and why it is not an easy problem to solve. ***Please give us a minute of your time to answer a few questions about this week's Hacking Healthcare topics. We'll publish the results in an upcoming issue. Survey link follows the articles below.***

Welcome back to *Hacking Healthcare*.

1. **FDA Announces Digital Health Center of Excellence**. On September 22nd, the FDA announced the launch of the Digital Health Center of Excellence (DHCoE). Described as part of the "planned evolution of the Digital Health Program in the Center for Devices and Radiological Health (CDRH)," the DHCoE's broad goal is to "align and coordinate digital health work across the FDA," and will engage with "mobile health devices, Software as a Medical Device (SaMD), wearables when used as a medical device, and technologies used to study medical products."[1, 2]

   The DHCoE's more specific mission will be to provide "regulatory advice and support to the FDA's regulatory review of digital health technology,"[3] although it should be noted that DHCoE is not responsible for marketing authorization decisions. DHCoE's mission will include the goal of "fostering responsible and high-quality digital health innovation" and will provide services in functional areas such as:

   - Digital Health Policy, Technology Support, and Training
   - Medical Device Cybersecurity
   - Artificial Intelligence / Machine Learning

   The tentative plan for the DHCoE is to continue to evolve along a three-phase process. Currently in phase one, the DHCoE is primarily focused on raising awareness and engaging with stakeholders through activities like listening sessions. The transition to phase two is expected shortly and will prioritize building strategic partnerships, developing resources for stakeholders, and assembling advisory groups. Finally, from

the winter of 2021 onward, the DHCoE intends to enter phase three and continue to build out capacity.

Action & Analysis
H-ISAC Membership Required

2. **HIPAA Security Risk Assessment Tool Gets an Update.** In an effort to help organizations successfully carry out the security assessment required by the HIPAA Security Rule, the Office of the National Coordinator (ONC) and the Office of Civil Rights (OCR) developed and made freely available the Security Risk Assessment (SRA) tool. As described by the ONC, "the tool diagrams HIPAA Security Rule safeguards and provides enhanced functionality to document how your organization implements safeguards to mitigate, or plans to mitigate, identified risks."[4] The tool has proven to be popular, especially among the small and medium sized entities it was designed for, as well as with entities who may lack the resources to engage with a third-party for an outside assessment.

   Earlier this month, ONC and OCR published an update (Ver 3.2) to the SRA that "includes a variety of new features, such as improved navigation throughout the assessment sections, export options for reports, and enhanced user interface scaling."[5] The update should continue to make the SRA easier to use while providing the same comprehensiveness in assessing risk. The updated SRA version can be found at Healthit.gov and is currently available for Windows OS.

   Action & Analysis
   H-ISAC Membership Required

3. **Are You Adequately Prepared for Third-Party Risks?** According to new research from cyber services firm BlueVoyant, the answer is likely no. In research published last week, BlueVoyant shared some findings from their global study on third-party risk management. The findings paint a less-than-ideal picture of just how prepared organizations are to recognize and mitigate this type of risk.

   The study recorded the views of "1505 CIOs, CISOs and Chief Procurement Officers in organizations with more than 1000 employees across a range of vertical sectors," which included the healthcare sector.[6] While technically global, the study was limited to organizations in the United States, United Kingdom, Mexico, Switzerland, and Singapore.

   Some of the more significant findings are:[7]

   - "80% of organizations surveyed experienced a cybersecurity breach that originated from vulnerabilities in their vendor ecosystem in the past 12 months"
   - "29% say they have no way of knowing if cyber risk emerges in a third-party vendor"

- "Fewer than one-quarter (22.5%) monitor their entire supply chain"
- "32% only re-assess and report their vendor's cyber risk position either six-monthly or less frequently"
- "The average headcount in internal and external cyber risk management teams is 12"
- "81% say that budget for third-party cyber risk management is increasing, by an average figure of 40%"
- BlueVoyant found no dominant approach in tools used to manage third-party risk
- There was significant variation in risk by sector, with the business services sector suffering the highest rate of compromise and the manufacturing sector suffering the lowest rate

According to the feedback received from the study's participants, the three most recurring pain points organizations faced in operating third-party risk programs were: (1) managing the sheer number of alerts, (2) finding ways to address these issues with suppliers, and (3) determining how to prioritize risks.

Action & Analysis
H-ISAC Membership Required

Survey:

Please take one minute to answer a few questions about this week's Hacking Healthcare by visiting this link: https://www.surveymonkey.com/r/JRYC5P5

Congress –

Tuesday, September 22nd:
- No relevant hearings

Wednesday, September 23rd:
- No relevant hearings

Thursday, September 24th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU – No relevant hearings

September 29th, 2020

Sundries –

The price of stolen remote login passwords is dropping. That's a bad sign

https://www.zdnet.com/article/the-price-of-stolen-remote-login-passwords-is-dropping-thats-a-bad-sign/

Microsoft says it nixed China-linked hackers' apps from Azure cloud

https://www.cyberscoop.com/microsoft-apt40-gadolinium-azure/

Addressing Insider Threats with Event Triggers

https://www.nextgov.com/ideas/2020/09/addressing-insider-threats-event-triggers/168648/

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence
[2] https://www.fda.gov/news-events/press-announcements/fda-launches-digital-health-center-excellence
[3] https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence
[4] https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
[5] https://register.gotowebinar.com/register/1950973841861106956
[6]https://f.hubspotusercontent10.net/hubfs/4896063/Managing_3PR_Report_Press_Release.pdf?__hssc=246838043.1.1601306207907&__hstc=246838043.6fa3817bf060e1020b4cd2e7909f287f.1601306207906.1601306207906.1601306207906.1&__hsfp=1935073496&hsCtaTracking=1011d753-59d3-4406-bef3-823275738b4a%7Cdf64b51a-8274-4ed0-957d-5175015f4728
[7]https://f.hubspotusercontent10.net/hubfs/4896063/Managing_3PR_Report_Press_Release.pdf?__hssc=246838043.1.1601306207907&__hstc=246838043.6fa3817bf060e1020b4cd2e7909f287f.1601306207906.1601306207906.1601306207906.1&__hsfp=1935073496&hsCtaTracking=1011d753-59d3-4406-bef3-823275738b4a%7Cdf64b51a-8274-4ed0-957d-5175015f4728