Articles + Publications | October 7, 2020

FDA Launches Digital Center of Excellence and ONC Updates HIPAA Security Risk Assessment Tool

SPEAKERS

Judith L. O'Grady | Miranda Hooker | Sharon R. Klein | Alex C. Nisenbaum | Karen H. Shin

Who Needs to Know

Health Care and Life Sciences Organizations

Why It Matters

In order to safeguard their information, health care and life science organizations should remain vigilant in monitoring DHCoE developments and initiatives, including any policy/regulation clarifications related to digital health. They also should consider reviewing the SRA Tool to help conduct security risk assessments to better protect the personal health data entrusted to them.

In addition to the California governor's signing of AB-713, which provides more CCPA health-related exemptions, the U.S. Food and Drug Administration (FDA) and the Office of the National Coordinator (ONC) recently made new advancements to help health care and life science organizations comply with their regulatory obligations amid the COVID-19 pandemic. It is appropriate that the security assessment update coincided with the launch of the FDA's Digital Center of Excellence as digital health and the internet of things depends on the security of data subjects' personal information to ensure a level of trust.

FDA Digital Center of Excellence Launch

On September 22, the FDA announced the launch of the Digital Health Center of Excellence (DHCoE) within the Center for Devices and Radiological Health (CDRH). The DHCoE will provide regulatory advice and support to the FDA's regulatory review of digital health technology, which includes categories, such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine.

More specifically, the DHCoE will (1) help set digital health regulatory science research priorities for the CDRH; (2) coordinate research in mutual areas of interest for other FDA centers; (3) work toward developing a knowledge hub of tools and information for policy development and implementation; (4) work toward developing a one-stop-shop for digital health-related inquiries, as well as partnerships and collaborations; (5) create a network of digital health experts to share knowledge and expertise with the FDA; (6) tailor the FDA's oversight of digital health technology by reimagining its regulatory approach to Software as a Medical Device (SaMD) (*e.g.,* Software Precertification Pilot Program), and (7) explore how to leverage the unique benefits of Artificial Intelligence and Machine Learning in SaMD. The DHCoE, however, will not make marketing authorization decisions.

The DHCoE launch is part of the planned evolution of the CDRH's Digital Health Program, and will require

guidance given the sharp increase in telehealth and digital health programs due to the ongoing COVID-19 pandemic. Currently, 46% of patients now replace in-person visits with telehealth — up 11% from 2019. Moving forward, virtual visits could potentially account for $250 billion (or about 20%) of what Medicare, Medicaid, and commercial insurers spend on outpatient, office, and home health visits.[1]

HIPAA Security Risk Assessment Tool Update

With security threats like ransomware increasing[2] and with cybercriminals targeting high-revenue organizations like those in the health care sector, on September 14, the ONC and the Office of Civil Rights (OCR) released an update to the Department of Health and Human Services' (HHS) Security Risk Assessment (SRA) Tool. The organizations designed the tool to support and guide small- and medium-sized health care providers in complying with their risk assessment obligations under the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

Last updated in October 2018, the free resource helps organizations in four key ways: (1) to identify potential threats (*e.g.,* cyberattacks and theft) and vulnerabilities (*e.g.,* weak login to access EHR) to develop mitigation plans protecting electronic patient data; (2) to review all electronic devices that store or capture electronic-protected health information (ePHI) by adding documentation that details the organization's risk identification and analysis process (*e.g.,* vulnerability scans, site walk-throughs); (3) to assess overall security risks routinely; and (4) to uncover potential weaknesses in organizational security policies, process, and systems.

SRA Tool updates include new features, such as an enhanced user interface, custom assessment logic, modular workflows, progress tracker, detailed reports, ratings of threats and vulnerabilities, and a business associate and asset tracking tool. These updates follow the OCR's Summer 2020 Cybersecurity Newsletter, which highlights best practices for developing IT asset inventories to track the ePHI's location for covered entities and business associates.

Before the OCR newsletter, other organizations provided cybersecurity best practice guidance for the health care industry. In 2018 and 2019, the Health Sector Coordinating Council (HSCC) partnered with several government agencies, including the HHS and FDA, to release guidance documents for health care organizations, seeking guidance to increase their cybersecurity protections and/or respond to data breaches. Further on September 30, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center released a joint Ransomware Guide, which provides best practices for ransomware prevention, as well as a ransomware response checklist, serving as a ransomware-specific addendum to organization cyber incident response plans.

To safeguard their information, health care and life science organizations should remain vigilant in monitoring DHCoE developments and initiatives, including any policy/regulation clarifications related to digital health. They also should consider reviewing the SRA Tool to help conduct security risk assessments to better protect the personal health data entrusted to them.

[1] American Medical Association, *After COVID-19, $250 Billion in Care Could Shift to Telehealth*, https://www.ama-assn.org/practice-management/digital/after-covid-19-250-billion-care-could-shift-telehealth (June 18, 2020).

[2] According to the FBI's 2018 and 2019 Internet Crime Reports, we have seen a 37% annual increase in security threats and a 147% annual increase in associated losses from 2018 to 2019. Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (October 1, 2020).

RELATED INDUSTRIES + PRACTICES

- Digital Health
- Health Care + Life Sciences