4/28/25 WEDI FEDERAL UPDATE

OCR Settles HIPAA Ransomware Cybersecurity Investigation with Public Hospital. The Office for Civil Rights (OCR) announced a settlement with a public hospital on the U.S. Territory, island of Guam following two complaints alleging improper disclosure of electronic protected health information (ePHI) through a ransomware attack affecting approximately 5,000 individuals. OCR's investigation found that the hospital had failed to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to its ePHI. The hospital will implement a corrective action plan, be monitored by OCR for three years, and pay a fine of $25,000 under the terms of the resolution agreement. Go here to access the resolution agreement and corrective action plan.

Breach from Phishing Attack Results in OCR Settlement for Health Care Network. The settlement, announced by OCR, comes after an investigation into a potential violation by a California-based health care network from a phishing attack that exposed unsecured ePHI. The breach was reported in January 2020 following a phishing attack in June 2019. Nearly 200,000 individual's ePHI was compromised including their names, addresses, dates of birth, driver's license numbers, Social Security numbers, diagnoses, lab results, medications, treatment and claims information, and financial information. OCR's investigation found that the entity failed to use or disclose PHI only as permitted, conduct a thorough risk analysis, and notify affected individuals within 60 days of its discovery. The health care network has agreed to implement a corrective action plan that will be monitored by OCR for two years and pay a $600,000 settlement. Go here to access the resolution agreement and corrective action plan.

House Committee Leaders Question 23andMe Data Security Following Bankruptcy. Congressman Brett Guthrie (R-KY), Chairman of the House Committee on Energy and Commerce, Congressman Gus Bilirakis (R-FL), Chairman of the Subcommittee on Commerce, Manufacturing, and Trade, and Congressman Gary Palmer (R-AL), Chairman of the Subcommittee on Oversight and Investigations, sent a letter to 23andMe questioning the handling of consumers' sensitive data through a potential sale of the company or the data. Privacy concerns have been widespread since the company announced it had filed for bankruptcy in March 2025. While its data use and privacy statements are detailed, it is unclear if they will be upheld in a potential purchase of the data.

Surescripts Designated as Newest QHIN. Surescripts Health Information Network is the latest Qualified Health Information Network (QHIN) to achieve designation status by The Sequoia

Project. The Sequoia Project was named by the federal government as the Trusted Exchange Framework and Common Agreement (TEFCA) Recognized Coordinating Entity. As a QHIN, Surescripts Health Information Network exchanges data nationwide under the policies and requirements of TEFCA, which enables secure and timely messaging of patient health information in support care delivery.

Payer-to-Payer FHIR API Compliance Readiness Checklist Released. The Sequoia Project published a "Payer-to-Payer Compliance Readiness Checklist" to support payers in meeting the compliance deadline of the payer-to-payer requirements of the CMS Promoting Interoperability and Improving Prior Authorization Final Rule (0057-F). This new resource guides payers through regulatory requirements for payer-to-payer exchange of a patient's health information, including the application programming interface (API) interaction, data content, education, member consent, payer identification, and privacy and security. Under the Final Rule, impacted payers must support this exchange of data by January 1, 2027.

NIST's National Cybersecurity Center of Excellence Hosting a Cybersecurity and Privacy of Genomic Data Workshop on May 20. The National Institute of Standards and Technology (NIST) is holding a hybrid event on cybersecurity and privacy of genomic data on May 20. The event will include discussions on genomic data cybersecurity, genomic data privacy, and threat modeling. The deadline for registering for in-person attendance is May 13. Go here to review the agenda and register for the event.

CISA Releases Guidance on Potential Legacy Cloud Compromise. The Cybersecurity and Infrastructure Security Agency (CISA) released guidance to assist organizations and individuals that may be affected by a potential unauthorized access to a legacy cloud environment. While the scope and impact of the breach is currently unconfirmed, credential material, such as usernames, passwords, authentication tokens, etc., may be exposed, reused across unaffiliated systems, or embedded. The guidance provides recommendations to limit the risk of potential compromise, including resetting passwords, reviewing software infrastructure, and monitoring authentication logs.

Reminder: May 1 Deadline for Submitting Recommendations for Future MIPS Quality and Cost Measures. May 1 is the deadline to submit to the Centers for Medicare & Medicaid Services (CMS) quality and cost measures for consideration for future years of the Merit-based Incentive Payment System (MIPS). This opportunity allows clinicians and professional associations to provide input on future measures, including those in the quality performance and cost performance categories. Interested parties can submit quality and cost measures for CMS's consideration by completing the required fields and submitting applicable measure specifications via the CMS Measures Under Consideration Entry/Review Information Tool (MERIT).