OCR Settles Ransomware Cybersecurity Investigation for $500,000. The Office for Civil Rights (OCR) announced a settlement with a plastic surgery practice in South Dakota for several potential violations of the HIPAA Security Rule, following an investigation into a ransomware attack breach. OCR initiated an investigation following the receipt of a breach report filed by the practice in July 2017, which reported that it discovered that nine workstations and two servers were infected with ransomware, affecting the protected health information of 10,229 individuals. The credentials the hacker(s) used to access the practice's network were obtained through a brute force attack (hacking method that uses trial and error to guess passwords, login information, encryption keys, etc.) to their remote desktop protocol. After discovering the breach, the plastic surgery practice was unable to restore the affected servers from backup.

OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level; implement procedures to regularly review records of information system activity; and implement policies and procedures to address security incidents.

Under the terms of the settlement, the practice paid $500,000 to OCR and agreed to implement a corrective action plan that requires them to take steps to resolve potential violations of the HIPAA Security Rule and protect the security of electronic protected health information, including: (i) Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; (ii) Implement a written risk management plan to address and mitigate security risks and vulnerabilities identified in the Risk Analysis; (iii) Implement policies and procedures to address security incidents, including a process for: identifying and responding to known security incidents; mitigating, to the extent practicable, harmful effects of known security incidents; and documenting (in writing) security incidents and their outcomes; (iv) Implement policies and procedures to establish methods to create and maintain retrievable exact copies of ePHI, including a process to: test the recoverability of backups on a regular basis to ensure that a retrievable exact copy will be available; create and maintain multiple copies of encrypted backups; and securely store backups in differing locations; (v) Implement policies and procedures to verify that a person or entity seeking access to ePHI is the one claimed; (vi) Implement policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights; (vii) Revise its policies and procedures relating to the uses and disclosures of PHI to ensure that its workforce members understand: 1) the circumstances under which PHI may be used and disclosed; 2) how to identify situations that constitute impermissible uses and disclosures of PHI; and 3) how and when to report situations that might constitute impermissible uses and/or disclosures of PHI; (viii) Revise its Breach Notification policies and procedures to ensure that its workforce members understand that, following a breach of unsecured PHI, affected individuals must be notified without unreasonable delay and in no case later than 60 (sixty) calendar days after the discovery of the breach, and that notification must be

made to the HHS Secretary and, in certain circumstances, to the media; and (ix) Provide training to its workforce on HIPAA policies and procedures. Go here to read the resolution agreement and corrective action plan.

HIPAA Modifications Proposed Rule Goes to OMB for Final Review. The proposed rule titled "Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information" has been sent to the Office of Management and Budget (OMB) for review. According to the listing in the Spring Unified Agenda, this rule will propose modifications to the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). These modifications will improve cybersecurity in the health care sector by strengthening requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats. Traditionally, OMB has up to 90 days to review a rule prior to its release for public comment. WEDI expects to host a Member Position Advisory (MPA) event once the proposed rule is published to gather member input on what is expected to be a landmark regulation.

CMS Releases PFS Final Rule, Includes Payment Cut. The Centers for Medicare & Medicaid Services (CMS) has issued its Calendar Year (CY) 2025 Medicare Physician Fee Schedule (PFS) Final Rule, finalizing changes for Medicare payments under the PFS and other Medicare Part B policies, effective on or after January 1, 2025. Key policy provisions included in the Final Rule are:

- For CY 2025, the average payment rates under the PFS will be reduced by 2.93% in CY 2025, compared to the average amount these services were paid for most of CY 2024. The change to the PFS conversion factor incorporates the 0% overall update required by statute, the expiration of the temporary 2.93% increase in payment for CY 2024 required by statute, and a relatively small estimated 0.02% adjustment necessary to account for changes in work relative value units (RVUs) for some services. This amounts to an estimated CY 2025 PFS conversion factor of $32.35, a decrease of $0.94 (or 2.83%) from the current CY 2024 conversion factor of $33.29.
- For CY 2025, CMS finalized its proposal to add several services to the Medicare Telehealth Services List, including caregiver training services on a provisional basis and PrEP counseling and safety planning interventions on a permanent basis. CMS is also finalizing to continue the suspension of frequency limitations for subsequent inpatient visits, subsequent nursing facility visits, and critical care consultations for CY 2025. Further, beginning January 1, 2025, CMS finalized that an interactive telecommunications system may include two-way, real-time, audio-only communication technology for any Medicare telehealth service furnished to a beneficiary in their home, if the distant site physician or practitioner is technically capable of using an interactive telecommunications system, but the patient is not capable of, or does not consent to, the use of video technology.

- For the Merit-based Incentive Payment System (MIPS), CMS finalized policies for the 2025 performance period for the MIPS performance categories, adding 7 new quality measures, substantive changes to 66 quality measures, the removal of 10 quality measures, and various other MIPS provisions. CMS also maintained the current performance threshold policies, leaving the MIPS performance threshold set at 75 points for the 2025 performance period.
- For the MIPS Value Pathways (MVPs), CMS finalized 6 new MVPs for the 2025 performance period that are related to ophthalmology, dermatology, gastroenterology, pulmonology, urology, and surgical care. The agency also finalized limited modifications to the previously finalized MVPs, including the consolidation of 2 neurology-focused MVPs into a single neurological MVP.
- CMS modified its Electronic Prescribing for Controlled Substances (EPCS) policy for a Covered Part D Drug Under a Prescription Drug Plan or a Medicare Advantage Prescription Drug Plan. The agency finalized its proposal to extend the date after which prescriptions written for a beneficiary in a long-term care (LTC) facility would be included in determining the CMS EPCS Program compliance, from January 1, 2025, to January 1, 2028, and that related non-compliance actions would commence on or after January 1, 2028.
- CMS finalized policies to establish a new "prepaid shared savings" option to encourage investments by eligible Accountable Care Organizations (ACOs) that have a history of earning shared savings that would aid beneficiaries, such as investments in direct beneficiary services and investments to improve care coordination through enhanced staffing or health care infrastructure. CMS is also finalizing changes to the Shared Savings Program's financial methodology to encourage ACO participation in the Shared Savings Program, by removing barriers for ACOs serving underserved communities and increasing incentives to enter and remain in the program, through the application of a health equity benchmark adjustment. Additionally, the agency finalized several policies to align quality measure reporting with the Adult Universal Foundation Measures (Universal Foundation) and promote digital quality measure reporting.

MSSP Reports more than $2 Billion in Savings. The Centers for Medicare & Medicaid Services (CMS) announced that the Medicare Shared Savings Program (MSSP) yielded more than $2.1 billion in net savings in 2023 — the largest savings in the Shared Savings Program's history. In addition, CMS reported that Accountable Care Organizations (ACOs) in the Shared Savings Program earned shared savings payments (also known as performance payments) totaling $3.1 billion, the highest since the program's inception more than 10 years ago. ACOs scored better on many quality measures than other types of physician groups and continued to demonstrate quality improvement. ACOs led by primary care clinicians had significantly higher net per capita savings than ACOs with a smaller proportion of primary care clinicians. Go here for more information on the MSSP.

OIG Issues Report Calling for Oversight of Remote Patient Monitoring in Medicare. The Office of the Inspector General (OIG) released a report calling for additional oversight of remote patient monitoring (RPM) to ensure that is being used

appropriately and that Medicare is billed properly. The OIG found that: (i) The use of remote patient monitoring in Medicare increased dramatically from 2019 to 2022; (ii) About 43 percent of enrollees who received remote patient monitoring did not receive all 3 components of it, raising questions about whether the monitoring is being used as intended; (iii) OIG and the Centers for Medicare & Medicaid Services (CMS) have raised concerns about fraud related to remote patient monitoring; and (iv) Medicare lacks key information for oversight, including who ordered the monitoring for the enrollee.

In the report, OIG made the following recommendations: (i) Implement additional safeguards to ensure that remote patient monitoring is used and billed appropriately in Medicare; (ii) Require that remote patient monitoring be ordered and that information about the ordering provider be included on claims and encounter data for remote patient monitoring; (iii) Develop methods to identify what health data are being monitored; (iv) Conduct provider education about billing of remote patient monitoring; and (v) Identify and monitor companies that bill for remote patient monitoring.

ASTP/ONC Details Information Blocking Reminders Related to API Technology. In a blog post, the Assistant Secretary for Technology Policy, Office of the National Coordinator for Health IT (ASTP ONC) related concerns it has heard from individuals and organizations who use API technology. The agency details that certain API-related practices could implicate the information blocking regulations. ASTP ONC shares reminders regarding such API-related practices by health care providers and developers of certified health IT that may implicate the regulations. As well, ASTP ONC released a new fact sheet that also presents reminders about the relationship between API technology and the information blocking regulations.

HHS 405(d) Publishes New Poster on Security Operations and Incident Response. The Department of Health and Human Services' (HHS') 405(d) Program, a public-private partnership focused on improving the nation's cybersecurity, published a new poster focused on Security Operations and Incident Response. The poster emphasizes the importance of implementing a strong Security Operations Center (SOC) and an effective Incident Response (IR) process. An SOC can assist organizations mitigate attacks and appropriately react to cybersecurity threats. Deploying an IR process can assist organizations take fast action to reduce the potential impact of an attack and help restore systems. Health care organizations are encouraged to leverage this poster to improve their cyber hygiene.

HSCC Releases Survey to Measure Public Health Cybersecurity Readiness. The Health Sector Coordinating Council Cybersecurity Working Group (HSCC) released a survey aimed at measuring the cybersecurity readiness of the public health sector. The Public Health Cybersecurity Readiness Survey has been developed to improve the cybersecurity preparedness of state, local, tribal, and territorial (SLTT) public health agencies. Survey results will assist in developing recommendations for federal grant funding and influence policies within the public health sector. High levels of participation are crucial for gathering the data needed to inform recommendations for investments

and policy adjustments aimed at bolstering cybersecurity in public health. Answers will be kept anonymous, and the survey will be available until Dec. 2. Access the survey here.

NIST to Host Public ARIA Program Workshop. The National Institute of Standards and Technology (NIST) will host a public workshop for its Assessing Risks and Impacts of AI (ARIA) program. The workshop will take place on November 12, 2024, from 10 am – 4:30 pm. ARIA is a NIST AI Innovation Lab program to gather evidence about AI's risks to people and society as part of advancing the science and practice of AI risk measurement. Participants will learn about ARIA's experimentation environment and NIST's approach to evaluation-driven research. This is the first in a series of ARIA workshops to facilitate discussion about aspects of this unique program. The series will begin with a deep dive into the role of annotation in the ARIA program. The target audience for this workshop is any organization currently participating (or interested in participating) in the ARIA pilot efforts, those working in the field of socio-technical evaluations, and organizations engaged in the annotation of human-AI interactions. Go here to register for the virtual attendance option.