# 6/23/25 WEDI FEDERAL UPDATE

**WEDI Submits Comments to HHS on the CMS and ASTP/ONC Health Technology Ecosystem RFI.** WEDI submitted comments to the Department of Health and Human Services (HHS) on the Centers for Medicare & Medicaid Services (CMS) and Assistant Secretary for Technology Policy (ASTP)/Office of the National Coordinator for Health Information Technology (ONC) (collectively, ASTP/ONC) "Health Technology Ecosystem Request for Information" (RFI). The RFI sought input from the public regarding the market of digital health products for patients, the state of data interoperability and broader health technology infrastructure, and responsible adoption of technology. In response to the RFI, WEDI held a Member Position Advisory (MPA) facilitated discussion of the questions and input from the MPA was used in developing WEDI's comments.

Special thanks to the MPA facilitators: Merri-Lee Stine (Aetna, a CVS Company, WEDI Board Chair); Denny Brennan (MHDC, WEDI Board Chair-Elect); Gail Kocher (BCBSA, WEDI Board Director); Heather McComas (AMA; WEDI Board Director); Michelle Barry (Availity; Co-Chair, Provider Information SWG); Stanley Nachimson (Nachimson Advisors; Co-Chair, Claims SWG, No Surprises Act TG); Samantha Burch (AHIP); Jeff Coughlin (AMA); Alix Goss (Point of Care Partners); Michael Phillips (CAQH); and moderator Nancy Spector (WEDI). WEDI supported the direction of the RFI and called on CMS and ASTP to ensure health information needs of the patient are prioritized; promote seamless, automated data exchange using mature standards; and integrate data exchange efficiently within the health plan, provider, and other end-users' workflows.

**Bipartisan Cybersecurity Legislation Introduced in the House.** Representative Brian Fitzpatrick (R-PA), Chairman of the CIA Subcommittee on the House Permanent Select Committee on Intelligence (HPSCI), and Representative Jason Crow (D-CO) introduced the Healthcare Cybersecurity Act (bill text). The bill is supported in the Senate by Senators Jacky Rosen (D-NV) and Todd Young (R-IN). If enacted, the bill would: (i) Require the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Health and Human Services (HHS) to coordinate efforts to identify and mitigate cybersecurity threats to the healthcare and public health sectors;(ii) Establish a formal liaison between CISA and HHS to improve communication, threat analysis, and incident response; (iii) Authorize cybersecurity training for healthcare

providers and personnel; and (iv) Direct both agencies to conduct a joint study identifying specific cybersecurity vulnerabilities and risks within the sector.

**CMS Issues Hospital Price Transparency RFI.** CMS issued a Request for Information (RFI) seeking public input on whether and how the agency can improve hospital price transparency (HPT) compliance and enforcement processes to ensure that the hospital pricing data in the machine-readable file is accurate and complete. This RFI relates to the President's Executive Order 14221, to ensure compliance with the transparent reporting of complete, accurate, and meaningful HPT data. Responses are due to CMS by July 21.

**Newly Created Remote Monitoring Leadership Counsel Advocates for RPM Use.** Several digital health companies have come together in the creation of the Remote Monitoring Leadership Council (the Council) to advance remote patient monitoring (RPM) technology. The Council's focus is on increasing access to RPM services for patients to enable improved health outcomes and reduced costs. Members of the Council are Best Buy Health, Biofourmis, BioIntelliSense, Cadence, CoachCare, CopilotIQ, HealthSnap, and impilo. Principles set by the Council include using RPM to support continuity of care, supporting patients in their health care, providing evidence-based RPM services, using patient health data appropriately, and promoting use of RPM for patients.

**NIST Outlines the Impact of AI on Cybersecurity Workforce.** The National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) published a blog outlining how artificial intelligence (AI) is reshaping the cybersecurity workforce. The post is based on NIST collaboration with government, industry, academia, and international partners, NICE is exploring how AI technologies impact cybersecurity job functions, skills, and strategic planning. NIST plans to integrate these insights into the NICE Workforce Framework for Cybersecurity (NIST SP 800-181 Revision 1), which was updated in 2020 to allow for more flexible revisions.

**FDA Launches AI Tool to Optimize Performance.** The U.S. Food and Drug Administration (FDA) launched Elsa, a generative AI tool designed to help agency employees such as scientific reviewers and investigators work more efficiently. Elsa, according to the agency, will modernize agency functions and leverage AI capabilities. Elsa is a large language model–powered AI tool designed to assist with reading and writing. It also can summarize adverse events to support safety profile assessments, perform faster label comparisons, and generate code to help develop databases for nonclinical applications.

**Joint Commission joins with CHAI on new AI Partnership.**

The Joint Commission, an independent, evidence-based health care standard setting organization, and the Coalition for Health AI (CHAI), a nonprofit organization founded by clinicians to advance responsible health AI, announced a new partnership to accelerate the development and adoption of AI best practices and guidance across the U.S. health care system. Together, the organizations will co-develop a suite of AI playbooks, tools, and a new certification program rooted in The Joint Commission's platform for evidence-based standards, and CHAI's consensus-based best practices for health AI. By bringing together CHAI's broad-based membership and expertise in safe AI, and the reach of The Joint Commission-accredited hospitals and health systems, the two organizations will set standards for AI adoption in health care. The first guidance will be available in Fall 2025, with AI certification to follow.

**JAMA Open Network Analysis Reports Ransomware Attacks and Data Beaches.** A research letter published in JAMA Network Open titled "Ransomware Attacks and Data Breaches in US Health Care Systems" reports on unauthorized releases of protected health information (PHI) through ransomware, hacking, and theft continually garner media attention. Analysis by researchers found that data breaches resulting in the exposure of PHI increased over 150% from 2010 (216 reports) to 2024 (566 reports). Of these breaches, hacking was the main cause. Ransomware attacks had not started in 2010; the first year of analysis by the researchers. By 2021, ransomware attacks accounted for 222 of 715 data breaches. This number dropped to 61 of 566 data breaches in 2024. Data breaches result in the potential exposure of patient records. From 2010 to 2024, approximately 732 million patient records were affected by various data breaches.