



12/15/25 WEDI FEDERAL UPDATE

WEDI Presents at CMS Listening Session on FHIR Prior Authorization Standard. WEDI presented at a hearing conducted by the Centers for Medicare & Medicaid Services (CMS) National Standards Group on the issue of the use of a FHIR® Standard for conducting prior authorization transactions. WEDI was invited to present along with the Designated Standards Maintenance Organizations: The Dental Content Committee; Health Level Seven; National Council for Prescription Drug Programs; National Uniform Billing Committee; National Uniform Claim Committee; and X12.

In developing our response to a series of seven questions posed by CMS, WEDI leveraged the information received at the November 17 WEDI member Position Advisory (MPA) event. Special thanks to the MPA facilitators Merri-Lee Stine (WEDI Board Chair), Denny Brennan (WEDI Chair-Elect), Janice Bakos (CVS Aetna), Samantha Burch (AHIP), Terry Cunningham (AHA), Beth Davis (Veradigm), Rajesh Godavarthi (MCG Health), Alix Goss (POCP), Gail Kocher (BCBSA), Michael Lunzer (Itility Health), Heather McComas (AMA), Cathy Shepard (X12), and Nancy Spector (Moderator, WEDI).

WEDI's recommendations to CMS included: (i) The FHIR implementation guides should be required, once a version is established following wide-spread industry experience; (ii) Long-term requirements to support multiple standards or multiple versions of one standard will increase industry cost; (iii) Providers will benefit from real-time responses, prior authorization policy transparency, and faster response times; (iv) CMS should establish a standardized process and cadence for FHIR updates (and other standards); and (v) CMS should conduct additional industry outreach with all impacted stakeholders prior to any rulemaking. Download the WEDI remarks [here](#).

FDA Launches TEMPO Digital Health Pilot for Chronic Disease Technologies. The Food and Drug Administration (FDA) [announced](#) the Technology-Enabled Meaningful Patient Outcomes (TEMPO) for Digital Health Devices Pilot, a voluntary pilot designed to promote access to certain digital health devices. The FDA is seeking statements of interest for participation beginning in January 2026. Up to 10 manufacturers in each of four specific clinical use areas will be selected to participate in the pilot. The pilot is being conducted in collaboration with the CMS Innovation

Center (CMMI) Advancing Chronic Care with Effective, Scalable Solutions (ACCESS) model. Participating manufacturers will offer digital health devices to provide care covered by the CMMI ACCESS model while collecting, monitoring, and reporting real-world performance data. TEMPO will evaluate how digital health technologies perform in real-life settings and how they may support efforts to improve care for people living with chronic diseases, including cardio-kidney-metabolic, musculoskeletal, and behavioral health conditions.

CMS 2025 QPP MIPS Exception Application Deadline is December 31. The deadline to submit an Extreme and Uncontrollable Circumstances (EUC) Exception application for the CMS 2025 Quality Payment Program (QPP) Merit-based Incentive Payment System (MIPS) is 8 pm ET on December 31. Participants in the program can submit their rationale for why they are unable to report data for one or more MIPS performance categories. To apply for an EUC exception, participants must sign in to their account on the [QPP website](#) and complete the questionnaire. Resources for submitting an EUC is available [here](#).

Bipartisan Senate Bill Reintroduced to Strengthen Health Care Cybersecurity. Senators Mark Warner (D-VA), Bill Cassidy, MD (R-LA), Maggie Hassan (D-NH), and John Cornyn (R-TX) reintroduced the [Health Care Cybersecurity and Resilience Act](#) to strengthen cybersecurity and protect health data. If enacted, the law would: (i) Provide grants to health care organizations to improve cyberattack prevention and response; (ii) Provide training cybersecurity best practices; (iii) Provide best practices to rural health providers on breach prevention, resilience, and coordination with federal agencies; (iv) Improve coordination between the Department of Health and Human Services (HHS) and Cybersecurity and Infrastructure Security Agency (CISA) to better respond to cyberattacks; (v) Modernize current regulations the Health Insurance Portability and Accountability Act; and (vi) Require the HHS Secretary to develop and implement a cybersecurity incident response plan. This legislation is an outcome of the senators' bipartisan health care cybersecurity working group launched in 2023.

Warning Issued of Cyber Attacks by Pro-Russia Hacktivists. CISA, in partnership with the Federal Bureau of Investigation, National Security Agency, and other federal and international partners, issued a joint cybersecurity advisory, "[Pro-Russia Hacktivists Create Opportunistic Attacks Against US and Global Critical Infrastructure](#)." The advisory, in conjunction to the joint fact sheet on [Primary Mitigations to Reduce Cyber Threats to Operational Technology \(OT\)](#) released in May, details that pro-Russia hacktivist groups are conducting less sophisticated, lower-impact attacks against critical infrastructure organizations. The attackers gain access to OT control devices using minimally secured, internet-facing virtual network computing (VNC) connections. The groups exploit accessible VNC devices to conduct the attacks. Organizations are advised to reduce their exposure of OT assets to the public-facing internet, adopt mature

asset management processes, and ensure that OT assets are using robust authentication procedures.

HHS Selects C3 AI to Develop AI Platform. C3 AI, an Enterprise AI application software company with the C3 Agentic AI Platform, [announced](#) that HHS has selected them to develop an AI data platform that will integrate data from the National Institutes of Health and CMS. The goal of the data platform is to combine various data sets, including diseases, claims, and state registries, to automate administrative functions, improve data quality, support research, and conduct analyses. Long-term, the data platform will support biomedical research, program integrity, and public health analysis.

CMS Contracts with CLEAR on Digital Identity Technology. CLEAR [announced](#) at an event, co-hosted by CMS, that it is contracting with CMS in its initiative to “[Kill the Clipboard](#),” which is one of the CMS’ Health Tech Ecosystem priorities. CLEAR1, CLEAR’s secure identity platform, will provide identity verification, account creation, and account recovery solutions for Medicare beneficiaries and providers. CLEAR has in operation check-in kiosks at several health care organizations that streamline the check-in process by confirming the patient’s identity using biometric data. CMS’ Kill the Clipboard initiative is focused on improving the patient verification process, addressing growing threats from AI, and closing current gaps in identity verification that plague health care. This work is expected to be integrated into CMS’ plans for a National Provider Directory for Medicare providers. Solutions using CLEAR’s technology are expected to be rolled out in 2026.

CHIME Releases 2025 Digital Health Most Wired Trends Report. The College of Healthcare Information Management Executives (CHIME) released its [Digital Health Most Wired: National Trends 2025 report](#), which measures the use of technology adoption in the advancement of health outcomes. The survey was completed by senior leaders in health care organizations of varying sizes and types, as well as national and international. The results focus on organizations’ efforts on infrastructure, cybersecurity, supply chain, administration, data analytics, interoperability, patient engagement, clinical quality, and innovation. Conclusions drawn from the survey data include: (i) The efficient use of technology, not just technology, is driving overall results; (ii) Organizations with measurable improvement are combining their use of governance, integration, and accountability; (iii) Organizations are becoming more seasoned in their use of digital technology and solutions; and (iv) The use of AI and automation need to be paired with trusted data and formal management processes.