7/7/25 WEDI FEDERAL UPDATE

CMS Introduces WISeR PA Model Aimed at Cutting Fraud, Waste, and Abuse. The Centers for Medicare & Medicaid Services (CMS) introduced a new model within the CMS Innovation Center called Wasteful and Inappropriate Service Reduction (WISeR). CMS will partner with companies and employ new technology, including artificial intelligence (AI), to address fraud, waste, and abuse in the Medicare program. The model will test methods to improve efficiency and expedite the prior authorization process (PA) with the goal of reducing unnecessary or inappropriate services for patients for select items and services that have been flagged for potential inappropriate use, as well as fraud and abuse. CMS has issued a Request for Applications for companies interested in participating in the WISeR Model.

Feds Release Fact Sheet Warning of Potential for Iranian Cyber Security Incidents. The Cybersecurity & Infrastructure Security Agency, along with the Federal Bureau of Investigation, Department of Defense Cyber Crime Center, and National Security Agency, released a fact sheet outlining potential threats of cyber security attacks in response to recent geopolitical events. The fact sheet specifically warns that Iranian threat actors may attack vulnerable U.S. networks, which have long been considered health care organizations. Recommendations in the fact sheet include: (i) Identifying and disconnecting operational technology from the public internet; (ii) Protecting devices and accounts with strong, unique passwords; (iii) Ensuring the latest software patches have been installed; and (iv) Implementing multifactor authentication where possible.

Proposed Ban on States' AI Laws Dropped from Final Budget Bill. A provision included in the House-passed budget bill that would have banned states from enacting laws applying to AI was eventually dropped from the bill passed by the Senate on July 1, and ultimately finalized by the House on July 3 by 218-214 and signed into law. The language in the initial House bill stated that no state could enforce any law or regulation related to AI models or systems for 10 years. The provision as written was widely unpopular as it would have significantly impacted current and planned uses of AI technology at state and local levels.

The new budget law did maintain steep cuts to Medicaid estimated at $1 trillion over ten years. The cuts will result in less funding provided to states from the federal government. The exact

impact on states' Medicaid programs is not yet known, but it has been widely projected that states will have budgetary shortfalls that will put pressure on their funding and may result in changes to eligibility and benefits, along with other resources provided by Medicaid agencies.

ASTP/ONC Releases SVAP-Approved Standards for 2025. The Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC) released updated standards and implementation specifications versions for use in the ONC Health IT Certification Program. These standards and implementation specifications were approved through the Standards Version Advancement Process (SVAP) following public input. These updates are available for use in the ONC Certification Program on August 29, 2025, and health IT developers can begin voluntarily incorporating them into their Certified Health IT Modules then. ASTP/ONC intends to all appropriate test data and tools with these updates.

CMS Innovation Center Releases Evaluation Reports for Payment Models. The CMS Innovation Center released various reports and findings of several payment models, including the Primary Care First Model, ACO REACH Model, Kidney Care Choices Model, and Bundled Payments for Care Improvement Advanced Model. The evaluations and research reports can be accessed on the website. In general, analysis of the models' data is used to identify changes and assess the overall success of them.

Open Payments Data Published by CMS for Program Year 2024. The Open Payments data for Program Year 2024 published by CMS shows that pharmaceutical and medical device companies reported a total of $13.18 billion in payments or transfers of value to health care providers during 2024. Open Payments collects and publishes information about financial relationships between the applicable companies and specific health care providers, including hospitals, physicians, physician assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists, anesthesiologist assistants and certified nurse midwives. The 2024 payments are attributable to three high-level categories with $3.33 billion in general payments, $8.52 billion in research payments, and $1.34 billion in ownership or investment interests. This national disclosure program promotes transparency and accountability and provides the public with information on payments and other transfers of value between these companies and health care providers.

The Sequoia Project Releases QTFv2.1 for Public Feedback. As the Trusted Exchange Framework and Common Agreement™ (TEFCA™) Recognized Coordinating Entity® (RCE®), the Sequoia Project is seeking feedback on its draft Qualified Health Information Network® (QHINTM) Technical Framework (QTF) Version 2.1 (QTFv2.1) until July 28. Both red-lined and clean versions of QTFv2.1 are available for review. The primary change in this draft is the

allowance of directed queries to a participant or subparticipant for any data exchange need. The draft also includes an update for QHIN reporting of monthly exchange volumes, accommodating data reporting by the RCE. Registration is now open for a call on Monday July 7 at 2pm ET with the RCE where the draft changes will be reviewed.

Survey Results Raise Concerns about Cyber Security Readiness in Rural Hospitals. Black Book Research published results from a survey that identifies vulnerabilities in small and rural hospitals. The survey was conducted to assess organizational readiness and capabilities of hospitals with less than 150 beds and attracted 187 respondents. Organizations responded that they do not meet National Institute of Standards and Technology Cybersecurity Framework (82%), have an insufficient cyber security infrastructure (73%), do not have a full-time cyber security leader (68%), lack continuous threat monitoring (59%), and have not completed a cyber security risk assessment in the past year (52%). Challenges reported by the respondents include inadequate staffing, funding, and infrastructure.