8/25/25 WEDI FEDERAL UPDATE

HHS Publishes Interim Final Rule Updating Compliance Dates for NCPDP Retail Pharmacy Standards. The U.S. Department of Health and Human Services (HHS) published an Interim Final Rule (IFR) updating the compliance and other dates for the National Council for Prescription Drug Programs (NCPDP) Retail Pharmacy Standards and the Medicaid Pharmacy Subrogation Standard. This IFR is subsequent to the "Administrative Simplification: Modifications of Health Insurance Portability and Accountability Act of 1996 (HIPAA) National Council for Prescription Drug Programs (NCPDP) Retail Pharmacy Standards; and Modification of the Medicaid Pharmacy Subrogation Standard" final rule that was published in the December 13, 2024, Federal Register (89 FR 100763) and correction notice published in the February 11, 2025, Federal Register (90 FR 9289). The February 2025 notice delayed the December 2024 final rule's effective date by 60 days to April 14, 2025, and acknowledged the impact of the delayed effective date on the compliance and transition period dates for covered entities and state Medicaid agencies. The IFR sets a new compliance date and transition period for HIPAA covered entities, as follows:

- Transition Period Starting August 14, 2027: Either NCPDP Version D.0 and Version 1.2 or Version F6 and Version 15 may be used by covered entities, as agreed by trading partners
- Compliance Date April 14, 2028: NCPDP Version F6 and Version 15 must be used by covered entities
- State Medicaid Agencies' Compliance Date: April 14, 2028

HHS Proposed FY2026 Budget Highlights Investments in Health IT. The proposed Fiscal Year (FY) 2026 budget, detailed in "Fiscal Year 2026 Budget in Brief," for HHS totals $94.7 billion in discretionary budget and includes reorganizations and investments in health information technology (IT). The budget plan funds a new Chief Technology Officer at $130 million, which is where the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC) will be located. HHS' work on health IT initiatives, including cybersecurity, will be led by ASTP/ONC and the Office of the Chief Information Officer. The focus on health IT will include development of policy, identification of technology standards, and advancement of interoperability.

HHS Seeking Nominations for New Advisory Committee. HHS and the Centers for Medicare & Medicaid Services (CMS) are seeking nominations for a new Healthcare Advisory Committee that will focus on developing strategic recommendations on improving the delivery and financing of Medicare, Medicaid, Children's Health Insurance Program, and the Health Insurance Marketplace. The committee will focus on: (i) Initiatives to promote chronic disease prevention and management; (ii) Accountability for safety and improved patient health; (iii) Advancement of a real-time data systems for claims processing and quality measurement; (iv) Opportunities to improve quality of care for vulnerable patients; and (v) Opportunities to modernize risk adjustment and quality measures to assess and improve health outcomes. The committee will be comprised of 15 individuals with expertise from various aspects of the health care system, including the medical field, manufacturing, government, academia, health insurance and payment programs, and health economics. Nominations are due by September 22 and are to be submitted via email to HAC@cms.hhs.gov.

OCR Settles HIPAA Ransomware Security Rule Investigation with New York Business Associate. The HHS Office of Civil Rights (OCR) announced a settlement with a New York accounting, consulting, and advisory firm for a potential violation of the HIPAA Security Rule. The firm, as a business associate, receives both financial and protected health information (PHI) from a HIPAA covered entity. OCR's investigation resulted from a breach report made by the firm in February 2020 after it became aware that a ransomware compromised its network in December 2019 and affected its covered entity client's PHI. According to OCR, the firm had not completed a thorough risk analysis to identify potential risks and vulnerabilities to the PHI within its systems. This settlement is OCR's 15th ransomware enforcement action and 10th enforcement action of the Risk Analysis Initiative. Under the terms of the resolution agreement, the provider agreed to implement a corrective action plan that OCR will monitor for two years and pay a fine of $175,000.

NIST Releases Outline for Zero Draft AI Standards. The National Institute of Standards and Technology (NIST) released an outline for a proposed "zero draft" standard for artificial intelligence (AI) testing, evaluation, verification, and validation. NIST is seeking feedback on the outline and comments received by September 12 will be considered for the initial public draft. The AI Standards Zero Drafts project is intended to speed AI innovation and address AI needs by piloting a process to improve standards development and broaden participation in the work. During NIST's work on AI standards, stakeholders have identified challenges with the process related to the need to speed development and engage experts not usually involved in standards development. NIST is addressing these challenges by releasing proposals, collecting input, and developing drafts for new project proposals. Feedback on the outline can be submitted to: ai-standards@nist.gov.

Justice Department Actions Lead to Seizure of Property and Disruption of Ransomware Operations. The Justice Department announced the seizure of four servers, nine domains, and over $1 million in virtual currency in a coordinated action against the BlackSuit (Royal) Ransomware group, a known serious threat to U.S. public safety. The operation was coordinated among the U.S. Department of Homeland Security, U.S. Secret Service, Internal Revenue Service Criminal Investigation unit, Federal Bureau of Investigation, and international law enforcement from the United Kingdom, Germany, Ireland, France, Canada, Ukraine, and Lithuania. The ransomware group has persistently attacked critical U.S. infrastructure, including health care and public health facilities, critical manufacturing, government facilities, and commercial facilities. This action demonstrates law enforcement's commitment to dismantling cybercriminal operations.

MedPAC Report Provides Insights on Medicare Utilization, Including ACOs, Telehealth, and APMs. The Medicare Payment Advisory Commission (MedPAC) July 2025 Data Book "Health Care Spending and the Medicare Program" (Data Book) provides comprehensive details on Medicare spending, services, and care settings. According to the data, 23% of Medicare beneficiaries are enrolled in Medicare Shared Savings Program Accountable Care Organizations (ACOs) and other ACOs and ACO-like models. Medicare beneficiaries used telehealth video and telephone services at a slightly lower rate than privately insured patients aged 50-64 and had similar rates of satisfaction. Although, the privately insured group was much higher, 61%, in their interest for using telehealth versus 44% of Medicare beneficiaries. The Data Book also provides details on providers' participation in Medicare. In 2024, over 380,000 providers qualified for the advanced alternative payment model (A-APM) participation bonus. The A-APMs are models in which the provider takes a financial risk and receives the bonus based on using a certified electronic health record (EHR) and achieving specific quality measures.

AMA Releases AI Toolkit to Assist Organizations with Governance and Policies. The American Medical Association (AMA), in collaboration with Manatt Health, has released a toolkit on augmented intelligence, commonly referred to as artificial intelligence, targeted for organizations implementing AI and developing governance and policies on its use. The toolkit, titled "Governance for Augmented Intelligence: Establish a Governance Framework to Implement, Manage, and Scale AI Solutions," provides a guide for provider organizations implementing AI. Covered in the governance framework are steps organizations can follow, including identifying responsibilities for leadership, establishing working groups, developing AI policies, identifying an oversight process, etc. The toolkit also includes definitions and concepts, challenges, decision-making and evaluation tools, and additional information useful for provider organizations implementing AI.