WEDI Submits Comments to ASTP/ONC on HTI-2 Proposed Rule. WEDI submitted **comments** on the proposed rule titled "Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability" (HTI-2) released by the Assistant Secretary for Technology Policy, Office of the National Coordinator for Health Information Technology (ASTP/ONC), Department of Health and Human Services (HHS). The WEDI comments were developed during the WEDI Member Position Advisory (MPA) event, held Sept. 12. Special thanks to the MPA facilitators, Jeff Coughlin (AMA), Terry Cunningham (AHA), Jay Eisenstock (JE Consulting), Cherie Holmes-Henry (NextGen), Gail Kocher (BCBSA), Danielle Lloyd (AHIP), and Arna Meyer (Albion Dental Technology Consulting).

CMS Issues New Admin Simp Compliance and Enforcement FAQs. The Centers for Medicare & Medicaid Services' (CMS) National Standards Group (NSG) has released new Administrative Simplification (Admin Simp) compliance and enforcement frequently asked questions (FAQs). The FAQs include answers to compliance and enforcement-related questions, including:

- What type of investigation does the National Standards Group (NSG) perform when it receives allegations of noncompliance with the HIPAA Administrative Simplification standards, operating rules, code sets, and unique identifiers?
- What is the Administrative Simplification Enforcement Tool (ASETT)?
- What information should I include when filing a HIPAA Administrative Simplification enforcement complaint?
- What should I expect after filing a HIPAA enforcement complaint using ASETT?
- Who can help me with issues with ASETT?
- What do I need to do to test a HIPAA transaction through ASETT?
- Do I need to provide Personally Identifiable Information (PII) when testing a HIPAA transaction using ASETT?
- I am trying to use ASETT to test transactions using ASC X12 5010 standards, but I am having trouble performing tests. What can I do?
- Where can I find educational materials regarding HIPAA Administrative Simplification transaction and code set enforcement on the CMS website?

Go here to access the full list of FAQs and here for additional resources on Admin Simp enforcement.

VA to Offer New Telehealth Options for Veterans to Get Emergency Care. The Department of Veterans Affairs (VA) announced that veterans can now leverage telehealth access emergency care from a Department of Veterans Affairs hospital under a new program that links patients experiencing medical distress with a VA provider. The VA stated that its tele-emergency care program, called tele-EC, is now available across the country, following a gradual rollout this year that has helped 61,182 veterans get care. According to the VA, nearly 60% of callers who contacted the department through the program had their health needs solved at home without requiring a visit to urgent care or an emergency room.

Veterans enrolled in VA health care contact VA Health Connect, which links them with a triage nurse who, in turn, connects them to a VA emergency physician if needed. The provider, who has access to a veteran's VA medical records, assesses the patient over the phone or by video and recommends treatment, follow-up or, in the case of a life-threatening emergency, calls 911 and stays on the line until emergency medical services arrive.

From 2016 through 2022, 3.9 million veterans made nearly 20 million visits to an emergency room, with roughly 73% going to the VA and the remainder landing in a civilian emergency department, according to research published earlier this year in JAMA Network Open. The study found that, from 2016 to 2022, the cost to the VA of visits by veterans to a civilian emergency room rose from $1.18 billion to $6.14 billion. The expectation is that the telehealth program will reduce the VA's emergency medical budget and also lower wait times in VA facilities as more veterans learn about it and use it.

NIST Launches Managing Cybersecurity and Privacy Risks in the Age of AI Program. In a blog post, NIH announced the launch of a new program for the cybersecurity and privacy of AI and the use of AI for cybersecurity and privacy. discusses how advancements in the broad adoption of AI may impact current cybersecurity and privacy risks, risk management approaches and how these risk management approaches relate to each other at the enterprise level. The program will focus on critical need for standards, guidelines, tools, and practices to improve the management of cybersecurity and privacy in the age of AI, ensure the responsible adoption of AI for cybersecurity and privacy protection purposes, and identify important actions organizations must take to adapt their defensive response to AI-enabled offensive techniques. Go here to learn more.

HC3 Issues Threat Briefing on Health Technology Security. The HHS' Health Sector Cybersecurity Coordination Center (HC3) issued a threat briefing covering Health Care Technology Security. Vulnerability management continues to be important for healthcare organizations – and they must secure both healthcare-specific technologies and universal technologies. The threat briefing outlines Common Vulnerabilities and Exposures (CVE) as well as security resources, and defense and mitigation strategies regarding Picture Archiving and Communication Systems (PACS) technology, the Digital Imaging and Communications and Medicine (DICOM) standard, medical devices, electronic health records (EHRs), and AI.

Registration Open for CMS Optimizing Healthcare Delivery Conference. CMS has announced that registration is now open for the 2024 CMS Optimizing Healthcare Delivery to Improve Patient Lives Conference taking place on December 12, 2024, from 11:00 AM to 4:00 PM ET. This free, virtual conference hosted by CMS will convene change makers from the healthcare community and federal government to share new ideas, lessons learned, and best practices to reduce administrative burden and strengthen access to quality care. Go here to register for the event.

New Bipartisan No Surprises Act legislation introduced. Representative Greg Murphy (R-NC) introduced the "Enhanced Enforcement of Health Coverage Act" (H.R.9572). The legislation is co-sponsored by Rep. Paul Ruiz, (D-CA), Rep. John Joyce (R-PA), Rep. Kim Schrier (D-WA), Rep. Jimmy Panetta (D-CA), and Rep. Ami Bera (D-CA). The bill seeks to close loopholes and assist patients within the No Surprises Act framework. In a press release, Murphy stated "In 2020, the bipartisan No Surprises Act was signed into law to put an end to surprise medical billing once and for all. Unfortunately, its implementation has been rife with unnecessary challenges. This legislation will reinforce the intent of the law and ensure the bipartisan process Congress established to protect patients from financial harm is effectuated. I'm grateful for my colleagues who have joined me in this bipartisan effort to prevent burdensome medical debt from crushing unexpecting patients any longer."

Senate Democrats Introduce Cybersecurity Standards Legislation. Senate Finance Committee Chair Ron Wyden (D-OR) and Senate Intelligence Committee Chair Mark Warner (D-VA) introduced the "Health Infrastructure Security and Accountability Act" (HISAA). HISAA seeks to modify and update the current HIPAA Security regulation to strengthen health care cybersecurity, deter cyberattacks, and be better prepared to recover from cyberattacks.

Key provisions include: (i) Requiring HHS to develop a new set of minimum cybersecurity standards for health care covered entities and business associates, along with enhanced standards for systemically important entities and entities important for national security; (ii) Impose user fees on entities that must comply with the new cybersecurity requirements to support HHS oversight and administration of the new cybersecurity standards; (iii) Require covered entities to undergo annual independent audits of their cybersecurity standard requirements and submit the audit reports to HHS agency; (iv) Require CEOs/CISOs to provide annual attestation of cybersecurity control compliance in their organization; (v) Require HHS to conduct yearly audits of at least 20 health entities overseen by those new rules; and (vi) Earmark $800 million over two years for 2,000 rural and urban safety net hospitals to adopt essential cybersecurity standards that address high risk cybersecurity vulnerabilities.