ASTP Publishes HTI-2 TEFCA Final Rule. The Assistant Secretary of Technology Policy (ASTP) published its Health Data, Technology, and Interoperability (HTI-2) Final Rule on the Trusted Exchange Framework and Common Agreement (TEFCA). ASTP states that HTI-2 Final Rule finalizes certain proposals related to TEFCA) from the HTI-2 Proposed Rule and seeks to advance interoperability and support the access, exchange, and use of electronic health information. The HTI-2 Final Rule amends the information blocking regulations by including definitions related to the TEFCA Manner Exception. According to the agency, the Final Rule also implements provisions to support the reliability, privacy, security, and trust within TEFCA.

The HTI-2 Final Rule finalizes a new part of the Code of Federal Regulations (CFR) for provisions related to TEFCA in 45 CFR Part 172. These final provisions further implement the Public Health Service Act section 3001(c)(9) as added by the Cures Act and provide greater transparency of TEFCA processes. The HTI-2 Final Rule also makes no changes to the TEFCA Manner Exception (§ 171.403) and adopts the TEFCA-related definitions as proposed. Access the Final Rule here. Additional HTI-2 rules are expected.

CMS Publishes Final Rule on NCPDP Retail Pharmacy Standards. The Centers for Medicare & Medicaid Services (CMS) published a Final Rule titled "Administrative Simplification: Modifications of Health Insurance Portability and Accountability Act National Council for Prescription Drug Programs Retail Pharmacy Standards; and Modification of the Medicaid Pharmacy Subrogation Standard." The Final Rule adopts updated versions of the retail pharmacy standards for electronic transactions adopted under the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The modifications adopted in the rule are named the NCPDP Telecommunication Standard Implementation Guide, Version F6 (Version F6) and equivalent NCPDP Batch Standard Implementation Guide, Version 15 (Version 15); and NCPDP Batch Standard Medicaid Subrogation Implementation Guide, Version 10. Version F6 and Version 15 are modifications to adopted standards for retail pharmacy transactions; Version 10 is a modification to the adopted standard for Medicaid pharmacy subrogation transactions.

OCR Imposes a $548,265 CMP Against Hospital for HIPAA Privacy and Security Rules Violations. The Office for Civil Rights (OCR) announced a $548,265 civil monetary penalty CMP against a hospital in Colorado. The action concerned violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules following receipt of breach reports in 2017 and 2020, relating to email phishing and cyberattacks.

OCR investigated the hospital following breaches which reported a phishing attack that compromised an email account containing 3,370 individuals' protected health information (PHI) and another after three email accounts were breached, containing 10,840 individuals' PHI. OCR's investigation determined that the first reported breach occurred because multi-factor authentication was disabled on an email account. The second breaches occurred, in part, when workforce members gave permission to unknown third parties to access their email accounts. OCR also found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems.

In June 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. The hospital waived its right to a hearing and did not contest OCR's findings. Accordingly, OCR imposed a civil money penalty of $548,265. Access the Notice of Proposed Determination here.

OCR Settles With Clearinghouse for $250,000. OCR announced a settlement with a health care clearinghouse concerning potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. OCR received a complaint that HIPAA protected health information was accessible to search engines like Google, on the internet.

In 2018, OCR received a complaint concerning PHI left unsecured on the internet. Following the initiation of OCR's investigation, the clearinghouse provided breach notification to HHS and affected individuals. OCR's investigation determined that from May 2016 through January 2019, the PHI of 1,565,338 individuals was made publicly available online. The PHI disclosed included patient names, dates of birth, home addresses, Social Security numbers, claims information, diagnosis/conditions and other treatment information. These impermissible disclosures of PHI were potential violations of the HIPAA Privacy Rule. The agency's investigation also identified multiple potential HIPAA Security Rule violations including: failures by the organization to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; and to monitor and review its health information systems' activity. The settlement resolves OCR's investigation concerning this HIPAA breach.

Under the terms of the settlement, the clearinghouse paid OCR $250,000. OCR determined that a corrective action plan was not necessary in this resolution as it had previously agreed to a settlement with 33 states that includes corrective actions that address OCR's findings in this matter. Go here to read the OCR resolution agreement.

IHS First Federal Agency to Join TEFCA. The eHealth Exchange, a Qualified Health Information Network (QHIN) under the Trusted Exchange Framework and Common Agreement (TEFCA) announced that The Indian Health Service (IHS) has selected it and is now exchanging health data via TEFCA. While other federal health agencies are evaluating their TEFCA strategies, IHS, an agency within the U.S. Department of Health and Human Services, is the first to go live with its data modernization efforts. IHS has been working with eHealth Exchange since 2011 when the network was originally formed. IHS provides care for approximately 2.8 million American Indians and Alaska Natives who belong to 574 federally recognized tribes in 37 states. IHS has 45 hospitals, including 19 critical access hospitals, 59 health centers and 32 health stations. IHS has been an eHealth Exchange participant since 2020 and has longstanding representation on the eHealth Exchange Coordinated Committee, a group of federal and non-federal participants who collectively provide governance, oversight, management, and support of the trust framework for eHealth Exchange network participants.

HSCC Publishes Cyber Incident Playbook. The Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group published a playbook to guide response to cyber incidents impacting medical product manufacturing and its operational technology (OT). The HSCC Joint Cybersecurity Working Group is a government-recognized critical infrastructure industry council of more than 470 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care.

The MPM-CIRP ("Playbook") provides step-by-step recommendations and processes for medical product manufacturers (principally medical device and pharmaceutical companies) to use in identifying and responding to manufacturing cyber incidents, from preparation through remediation. The recommendations and procedures are tailored to be applicable across organizations of various sizes and types and to provide a basic platform that organizations may use or adapt according to their own needs. This Playbook is meant to serve as a starting point—or accelerator—for companies to create and tailor their own internal playbooks for their specific circumstances. A portion of this product also demonstrates resourcefulness, in that it adapted its guidance from a similar effort done by the American Public Power Association in 2019. The authors accordingly give acknowledgement to that cross-pollinating critical infrastructure support. Go here to access the Playbook.

H-ARPA Initiate Program to Address AI Degradation. The Advanced Research Projects Agency for Health (H-ARPA), an agency located within the National Institute of Health (NIH) charged with conducting high-impact research to drive biomedical and health breakthroughs, has launched the PRECISE-AI program to address data degradation issues with artificial intelligence (AI) that can occur over time and can lead to negative patient outcomes. Currently, no clinical AI models undergo regular testing to ensure accuracy, and detection of degradation relies on clinical intuition, which is unreliable. The PRECISE-AI program aims to address this by developing tools to automatically detect and correct AI model degradation through tools used to monitor performance, identify degradation, and provide automatic corrections, reducing the burden on clinicians. The program will also improve communication about model uncertainty and degradation sources. H-ARPA has issued a solicitation surrounding this effort. Go here to learn how to become involved in this initiative.

ASTP Makes Available Recordings from its Annual Conference. ASTP held its annual meeting in Washington DC on Dec. 4-5. The event featured government and private sector speakers discussing the key issues at the intersection of health care, public health, policymaking, and technology. Several of the sessions reflected on the agency’s 20 year history and looked ahead to the future of better health enabled by health IT. Access the recordings here.