CMS Proposal Includes Changes to MA Plan HIT Policy. The Centers for Medicare & Medicaid Services (CMS) has released a Notice of Proposed Rulemaking entitled "*Medicare and Medicaid Programs: Contract Year 2026 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly*." Health IT (HIT) provisions in the rule include:

- Prior Authorization: Key proposals include defining the meaning of "internal coverage criteria" to clarify when MA plans can apply utilization management, ensuring plan internal coverage policies are transparent and readily available to the public, ensuring plans are making enrollees aware of appeals rights, and addressing after-the-fact overturns that can impact payment, including for rural hospitals. In addition, CMS stated that efforts are underway that will allow CMS to collect detailed information from initial coverage decisions and plan-level appeals, such as decision rationales for items, services, or diagnosis codes that will provide a better line of sight on utilization management and prior authorization practices, among many other issues.

  CMS also proposes to revise 42 CFR 422.112(a)(8) to require MA plans to ensure services are provided equitably, irrespective of delivery method or origin, whether from human or automated systems. The agency also clarifies that in the event that an MA plan uses AI or automated systems, they must comply with section 1852(b) of the Social Security Act and 42 CFR 422.110(a) and other applicable regulations and requirements and provide equitable access to services and not discriminate on the basis of any factor that is related to the enrollee's health status.

- Provider Directories: CMS is proposing that covered plans format provider directories for the Medicare Plan Finder (MPF). MPF is an online tool where current and prospective people with Medicare can explore their Medicare coverage options by comparing and shopping for Medicare Advantage and Part D plans. MPF allows individuals to shop around and make choices based on a variety of search criteria, such as plan benefits, premiums, deductibles, and Star Ratings. However, MPF does not currently include information on provider networks. Instead, CMS currently requires that MA organizations include on their plan websites a PDF or copy of a printable provider directory and a searchable provider directory, as well as provide a complete and accurate directory through a publicly accessible, standards-based Application Programming Interface. CMS proposes to further promote informed choice and transparency by requiring MA organizations to make provider directory data available to CMS to populate MPF.

- Artificial Intelligence: CMS proposes to require MA plans to "ensure services are provided equitably, irrespective of delivery method or origin, whether from human or automated systems." The agency clarifies that in the event that an MA plan uses AI or automated systems, they must comply with section 1852(b) of the Social Security Act and 42 CFR 422.110(a) and other applicable regulations and

requirements and provide equitable access to services and not discriminate on the basis of any factor that is related to the enrollee's health status.

OCR Settles with Hospital Over Disclosure of Patient's PHI. The Office for Civil Rights (OCR) announced a settlement with a Pennsylvania hospital concerning an alleged violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule due to an impermissible disclosure of a female patient's protected health information (PHI), including information related to reproductive health care. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records, requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization, (such as disclosures for health oversight activities or for law enforcement purposes), and gives individuals rights such as the ability to access their own medical records.

In September of 2023, OCR received a complaint alleging that thew hospital impermissibly disclosed a female patient's protected health information to the patient's prospective employer, including her surgical history, gynecological history, obstetric history, and other sensitive health information concerning reproductive health care. OCR's investigation found that the hospital disclosed the patient's full medical record, including protected health information concerning her reproductive health care, that it did not have the patient's authorization for the broad disclosure of her PHI, and that there otherwise was no applicable requirement or permission under the Privacy Rule for such a broad release of her medical records. The complainant stated that she had requested that the hospital send one specific test result, unrelated to her reproductive health, to a prospective employer.

Under the terms of the resolution agreement, the hospital paid $35,581 and agreed to implement a corrective action plan that requires them to:

- Submit a breach notification report to HHS regarding this incident;
- Review, develop or revise its policies and procedures to ensure compliance with the Privacy Rule, and submit all such policies and procedures to HHS for approval;
- Distribute all HHS-approved policies and procedures to its workforce and ensure that each member of the workforce certifies receipt and understanding of the policies and procedures;
- Train all members of its workforce on its HHS-approved policies and procedures, including all workforce members of its affiliated entities;
- Within 120 days after HHS approval of Holy Redeemers policies and procedures, the hospital must submit a written report to HHS detailing the status of its implementation of the corrective action plan;
- Provide a report to OCR regarding any non-compliance with its policies and procedures by any members of its workforce; and
- Provide annual reports to OCR regarding compliance with the corrective action plan.

Go here to read the resolution agreement and corrective action plan.

Bipartisan Legislation Introduced in the Senate to Strengthen Health Care Cybersecurity. Senators Bill Cassidy, M.D. (R-LA), ranking member of the Senate Health, Education, Labor, and Pensions (HELP) Committee, Mark Warner (D-VA), John Cornyn (R-TX), and Maggie Hassan (D-NH) introduced legislation to strengthen cybersecurity in the health care sector and protect health data. This legislation is a product of the senators' health care cybersecurity working group launched last year.

According to the sponsors, the Health Care Cybersecurity and Resiliency Act of 2024: (i) Strengthens cybersecurity in the health care sector by providing grants to health entities to improve cyberattack prevention and response; (ii) Provides training to health entities on cybersecurity best practices; (iii) Supports rural communities by providing best practices to rural health clinics and other providers on cybersecurity breach prevention, resilience, and coordination with federal agencies; (iv) Improves coordination between the Department of Health and Human Services (HHS) and Cybersecurity and Infrastructure Security Agency (CISA) to better respond to cyberattacks in the health care sector; (v) Modernizes current regulations so entities covered under the Health Insurance Portability and Accountability Act (HIPAA) use the best cybersecurity practices; and (vi) Requires the HHS Secretary to develop and implement a cybersecurity incident response plan. Click here for full bill text and click here for the section-by-section analysis of the bill.

DEA and HHS Extend Telehealth Flexibilities Until 2026. The U.S. Drug Enforcement Agency (DEA) and the Department of Health and Human Services (HHS) published in the Federal Register the "Third Temporary Extension of COVID-19 Telemedicine Flexibilities for Prescription of Controlled Medications." This action is designed to prevent some patients from losing access to their telehealth-prescribed medications. The third extension of pandemic-era telehealth flexibilities through the end of next year will give the federal government time to promulgate final regulations and providers time to comply, the agencies said. The agencies also said they would continue to develop the final rule governing the virtual prescribing of controlled substances in the post-pandemic era to be consistent with public health and safety and to mitigate drug diversion risks.

ASTP ONC Releases New Health IT Certification Program Fact sheet. The Assistant Secretary for Technology Policy (ASTP), Office of the National Coordinator for Health It (ONC) released a new fact sheet entitled "Promoting an Open and Transparent API Ecosystem: API Conditions and Maintenance of Certification Requirements for Certified API Developers in the ONC Health IT Certification Program." This fact sheet describes the application programming interfaces (APIs) requirements and expectations for Certified API developers participating in the Certification Program. It serves as a resource to help patients, clinicians, researchers, and other interested parties understand the requirements that apply to developers of Certified Health IT with products certified to any of the API certification criteria.

ASTP ONC Releases TEFCA Common Agreement Version 2.1. ASTP ONC published its "Notice of Publication of Common Agreement for Nationwide Health Information Interoperability (Common Agreement) Version 2.1" in the Federal Register. The updated version of the Trusted Exchange Framework and Common Agreement (TEFCA) Common Agreement Version 2.1 builds on the previous version's enhancements for efficiency. The agency contends it also increases transparency and trust by clarifying ASTP's role in helping to resolve Qualified Health Information Network (QHIN) disputes associated with use of exchange purposes. According to ASTP ONC, the Vetting Process Standard Operating Procedure (SOP) establishes the framework for assessing organizations seeking to participate in TEFCA and further enhances upfront trust and transparency within TEFCA.**CISA and FBI Release Ransomware Joint Advisory.** CISA, Federal Bureau of Investigation , and international partners released a joint advisory warning of cybercriminal activity by the BianLian ransomware group. The agencies stated that actions by BianLian actors have impacted multiple sectors across the U.S. since 2022. They operate by gaining access to victims' systems through valid remote desktop protocol credentials and use open-source tools and command-line scripting for finding and stealing credentials. The actors then extort money from organizations by threatening to release the stolen information. The Advisory suggests organizations take the following actions to mitigate cyber threats from BianLian data extortion: (i) Strictly limit the use of RDP and other remote desktop services; (ii) Disable command-line and scripting activities and permissions; and (iii) Restrict usage of PowerShell and update Windows PowerShell or PowerShell Core to the latest version.

Reminder: ASTP Annual Meeting Takes Place Dec. 4-5 in Washington, DC. The ASTP Annual Meeting is back in Washington, DC on December 4-5, 2024. The event will feature two days of conversation, learning, and networking. Attendees will hear about the key issues at the intersection of health care, public health, policymaking, and technology through a variety of keynote speakers and mainstage, breakout, and education sessions as ASTP ONC reflects on 20 years and look ahead to the future of health IT. Go here for more information and to register for the event.