ASTP ONC Finalizes Federal Health IT Strategy. The Assistant Secretary for Technology Policy, Office of the National Coordinator for Health Information Technology (ASTP ONC) published the final *2024-2030 Federal Health IT Strategic Plan* in accordance with the Health Information Technology for Economic and Clinical Health (HITECH Act.) The Strategic Plan presents federal health information technology (health IT) goals and objectives to achieve a future state where health IT and electronic health information are used to: (i) Promote health and wellness; (ii) Enhance the delivery and experience of care; (iii) Accelerate research and innovation; and (iv) Connect the health system with health data.

OCR Imposes a $240k CMP Following Ransomware Investigation. The Office for Civil Rights (OCR) announced a $240,000 civil monetary penalty (CMP) against a medical institute in Southern California, concerning potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, following a ransomware attack breach report investigation by OCR.

OCR initiated an investigation following the receipt of a breach report filed by the institute in April 2018, which reported that its systems were impacted by a series of ransomware attacks that affected the electronic protected health information (ePHI) of 85,000 individuals between February and March 2018. OCR's investigation determined that servers containing ePHI were encrypted with ransomware three times. OCR found two potential violations of the HIPAA Security Rule, including failure to have a business associate agreement in place and failure to implement policies and procedures to allow only authorized persons or software programs access to ePHI. Go here to read The Notice of Final Determination.

According to OCR, ransomware and hacking are the primary cyber-threats in health care. There has been a 264% increase in large breaches reported to OCR involving ransomware attacks since 2018. OCR recommends that health care providers, health plans, clearinghouses, and business associates that are covered by HIPAA take the following steps to mitigate or prevent cyber-threats: (i) Review all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident obligations; (ii) Integrate risk analysis and risk management into business processes; conducted regularly and when new technologies and business operations are planned; (iii) Ensure audit controls are in place to record and examine information system activity; (iv) Implement regular review of information system activity; (v) Utilize multi-factor authentication to ensure only authorized users are accessing ePHI; (vi) Encrypt ePHI to guard against unauthorized access to ePHI; (vii) Incorporate lessons learned from incidents into the overall security management process; and (viii) Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security.

Federal Agencies Mark October as Cybersecurity Month. Federal agencies including the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) are marking Cybersecurity Awareness Month. Resources include:

CISA

- Free Cybersecurity Awareness Month 2024 Toolkit includes new resources like tip sheets on how to stay safe online when using AI, reporting cybercrime, and raising digital citizens, as well as puzzles and posters.
- Participate in Cybersecurity Career Week from October 14-19th.
- Learn more about CISA's talent development initiatives aimed at filling the cyber workforce gap on October 16, 2024, at 2 p.m. ET. To register, click here.
- Partner with CISA's Secure Our World Program. To learn more, go to Secure Our World Opportunities Guide.
- Follow CISA on X, LinkedIn, Facebook, Instagram, and YouTube.

NIST

- NIST Cybersecurity Awareness Month website
- Be on the lookout for their blog posts throughout October. The first post can be found here.
- Check out their National Cybersecurity Center of Excellence (NCCoE) LinkedIn showcase page.
- They are hosting Cybersecurity Career Week during the week of October 14-19th. Click here for ways to participate.
- Follow NISTCyber on X as they spread the word about our various cybersecurity and privacy resources

HC3 Publishes "Malvertising" Warning. The Health Sector Cybersecurity Coordination Center (HC3) published a new Analyst Note on the issue of "Malvertising." According to HC3, this combination of "malicious" and "advertising" cyberattack method occurs where legitimate advertising networks are infiltrated with malicious advertisements. This tactic exploits digital advertising infrastructure to deliver malicious content to end users. These advertisements can appear on reputable websites and are designed to automatically infect devices with malware upon viewing or interacting with the ad. This form of attack leverages the trust users have in well-known websites, and ultimately exploits the complexity of the online advertising ecosystem. The Note details malvertising methods, impacts, and recommends mitigation strategies.

House Homeland Security Committee Advances 7 Cybersecurity Bills. The House of Representatives Homeland Security Committee, led by Chairman Mark Green (R-TN), advanced seven bipartisan cybersecurity bills. Legislation includes:

- H.R. 9770, the "Cyber PIVOTT Act," introduced by Chairman Green

- H.R. 9769, the “Strengthening Cyber Resilience Against State-Sponsored Threats Act,” introduced by Rep. Laurel Lee (R-FL)
- H.R. 3169, the “Identifying Adversarial Threats at our Ports Act,” offered by Subcommittee on Transportation and Maritime Security Chairman Carlos Gimenez (R-FL)
- H.R. 9469, the “Pipeline Security Act,” introduced by Rep. Robert Garcia (D-CA)
- H.R. 9689, the “DHS Cybersecurity Internship Program Act,” introduced by Rep. Yvette Clarke (D-NY)
- H.R. 9768, the “Joint Cyber Defense Collaborative Act,” introduced by Rep. Eric Swalwell (D-CA)
- H.R. 9762, the “DHS International Cyber Partner Act of 2024,” introduced by Rep. Robert Menendez (D-NJ)

ASTP ONC to Host Health IT Certification Program Developer Roundtable. ASTP ONC will host an ONC Health IT Certification Program Developer Roundtable on October 23, 2024. These public meetings are open to all health IT developers, regardless of their participation in the ONC Health IT Certification Program. During these meetings, ONC leads discussions tailored for the health IT developer community on topics such as Certification Program updates, upcoming certification deadlines, and developer requirements. For more information, including registration, please visit the ONC Events Page

ASTP ONC Publishes the 2024 SVAP Approved Standards. ASTP ONC released the Standards Version Advancement Process (SVAP) Approved Standards for 2024. These Approved SVAP Standards for 2024 are available for use in the ONC Health IT Certification Program. For more information on the newly approved SVAP standards, please visit the SVAP webpage, fact sheet, and blog.

Reminder: CMS to Host Webinar Oct. 21 on 2025 Hospital Price Transparency Requirements. The Centers for Medicare & Medicaid Services (CMS) will host a webinar on the 2025 hospital price transparency requirements on Monday, October 21, 2024, from 1–2:30 pm ET. As of July 1, 2024, hospital machine-readable files (MRFs) must conform to a CMS template layout and data specifications. Starting January 1, 2025, hospitals are also required to encode additional data elements. The webinar will cover: (i) How to encode the data elements required by January 1, 2025; and (ii) Tips to make sure your MRFs conform to the requirements effective July 1, 2024. Go here to register for the event.

More Information:

- Hospitals webpage
- Data Dictionary GitHub Repository:
    - Required CMS template layouts
    - Data dictionary
    - Examples of how to encode standard charges in the MRF
    - Q&A discussion board

- Tools webpage:
  - Online validator
  - Command-line interface validator
  - TXT file generator
  - MRF naming convention tool
- Resources webpage:
  - Final rules
  - FAQs
  - Guides
  - Webinar materials