OCR Settles 8th Ransomware Investigation. The Office for Civil Rights (OCR) announced an $80,000 settlement with a Massachusetts company that provides electronic medical record and billing support services to HIPAA covered entities. The settlement resolves an investigation concerning a ransomware attack on the vendor's information system. On March 25, 2023, an unknown actor gained access to a server on Elgon's information system through open ports on Elgon's firewall. Elgon did not detect the intrusion until March 31, 2023, when a ransom note was found. In June 2023, the vendor filed a breach report with HHS stating that approximately 31,248 individuals were affected when its computer system was infected with ransomware. The protected health information disclosed included demographic information (name, social security number, address, driver's license, and date of birth) and clinical information (medication, diagnosis, and condition).

OCR's investigation determined that the vendor failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI in its system. Under the terms of the settlement agreement, OCR will monitor the vendor for three years to ensure compliance with HIPAA. In addition, it has agreed to pay $80,000 to OCR and to implement a corrective action plan, which identifies the steps that it will take to resolve potential violations of the HIPAA Privacy and Security Rules and protect the security of electronic protected health information, including:

- Reviewing and updating its Risk Analysis to identify the potential risks and vulnerabilities to Elgon's data to protect the confidentiality, integrity, and availability of ePHI.
- Updating its enterprise-wide Risk Management Plan (strategy to protect the confidentiality, integrity, and availability of ePHI) to address and mitigate any security risks and vulnerabilities found in the updated Risk Analysis.
- Reviewing and revising, if necessary, its written policies and procedures to comply with the Privacy and Security Rules.
- Providing workforce training on HIPAA policies and procedures.

The resolution agreement and corrective action plan may be found here.

OCR Settles HIPAA Security Rule Investigation Concerning the Deletion of ePHI. OCR announced a $337,750 settlement with a business associate in Florida regarding a Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule issue. The settlement resolves a breach investigation concerning the deletion of electronic protected health information (ePHI) by an unauthorized third party.

OCR initiated an investigation following the receipt of a breach report filed by the business associate in February 2019, which reported that from August 23, 2018, through December 8, 2018, a database containing the ePHI of 2,903 individuals was accessed by an unauthorized third party/parties who were able to delete ePHI in the database. OCR's investigation found potential violations of the HIPAA Security and Privacy Rules, including failures to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; to regularly

review its information system activity; and to establish and implement procedures to create and maintain retrievable exact copies of ePHI. Under the terms of the settlement agreement, OCR will monitor the organization for two years to ensure compliance with HIPAA. In addition, it paid $337,750 to OCR and agreed to implement a corrective action plan that identifies specific steps it will take to resolve potential violations of the HIPAA Privacy and Security Rules and protect the security of ePHI, including:

- Conduct an accurate and thorough risk analysis to determine the potential risk and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis;
- Develop a process to evaluate any environmental or operational changes that affect the security of ePHI;
- Develop, maintain, and revise as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Distribute any updated HIPAA policies and procedures to its workforce.

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

FDA Publishes Draft Guidance on AI-Enabled Medical Device Software. The Food and Drug Administration (FDA) published in the Federal Register the availability of the draft guidance entitled ‘‘Artificial Intelligence Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations.’’ This draft guidance, when finalized, will provide recommendations regarding the contents of marketing submissions for devices that include artificial intelligence (AI)-enabled device software functions including documentation and information that will support FDA’s evaluation of safety and effectiveness. To support the development of appropriate documentation for FDA’s assessment of the device, this draft guidance also proposes recommendations for the design, development, and implementation of AI-enabled devices that sponsors may wish to consider using throughout the total product lifecycle. If finalized, the guidance would be the first to provide total product life cycle recommendations for AI-enabled devices, tying together all design, development, maintenance and documentation recommendations.

Congressional Taskforce Release AI Report. The U.S. House of Representatives Artificial Intelligence (AI) Taskforce released report that culminates its work over the past year. Headed by Representatives Jay Obernolte (R-CA) and Ted Lieu (D-CA) the Taskforce identifies 66 key findings and makes 85 recommendations for Congress to consider. The report includes a chapter on health care-outlining transparency, bias, privacy and security, interoperability, and other issues. The report notes that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rules may need to be updated to meet challenges created by AI systems. Access the report here.

CMS to Conduct Webinar Jan. 16 on No Surprises Act GFE Provision. The Centers for Medicare & Medicaid Services will host a webinar on Jan. 16 at 1 p.m. ET to provide an update to the industry on the No Surprises Act Good Faith Estimate (GFE)

requirements for uninsured and self-pay patients. (Note that CMS has not yet moved forward with requiring GFEs for insured individuals.) Agency staff will discuss recently-released Frequently Asked Questions on the GFE and focus on provider impact. Go here to register for the event

HC3 Publishes Credential Harvesting Alert. The Health Sector Cybersecurity Coordination Center (HC3) has released a new Sector Alert on Credential Harvesting. Credential harvesting involves attackers collecting sensitive login data to gain unauthorized access, leading to data theft, fraud, and system disruptions. Common methods include phishing, keylogging, man-in-the-middle attacks, credential stuffing, and social engineering. HC3 recommends educating employees on strong passwords, avoiding password reuse, recognizing phishing attacks, implementing multi-factor authentication, deploying email filters and endpoint security solutions, continuous system monitoring, and deploying regular software updates through vulnerability and patch management. Additionally, having a comprehensive incident response plan helps address and minimize the impact of credential harvesting incidents.

FTC Releases Preventing & Mitigating Digital Security Risks Tech Blog. The Federal Trade Commission (FTC) released a new post from its Office of Technology, titled “Lenses of Security: Preventing and mitigating digital security risks through data management, software development, and product design for humans.” FTC describes the importance of addressing systemic risks to protect consumers from data breaches and other security threats. The blog recommends organizations enforce data retention schedules, mandate data deletion, limit third-party data sharing, and encrypt sensitive information to enhance security and privacy. FTC also describes how the agency has addressed misrepresentations of security practices and misuse of security data. Access the blog here.

Sequoia Project Publishes TEFCA Governance SOP. The Sequoia Project, as the Trusted Exchange Framework and Common Agreement™ (TEFCA™) Recognized Coordinating Entity® (RCE®), published the TEFCA Governance SOP. This milestone Standard Operating Procedure (SOP) marks the transition to self-governance of TEFCA Exchange. The TEFCA Governance SOP details the creation of three permanent governing bodies, including a Governing Council, QHIN Caucus, and Participant and Subparticipant Caucus. It also establishes a mechanism for additional engagement through the creation of Advisory Groups. The RCE and the Governing Council may choose to use Advisory Groups in a variety of ways including, but not limited to, giving feedback on possible changes to the Common Agreement, the QTF, or an SOP; or providing feedback on new Exchange Purposes.

The interim TEFCA Transitional Council will finalize the establishment of the caucuses. The caucuses will then vote on the nominees for the Governing Council in the coming weeks. These new governing bodies will replace the Transitional Council. The existing TEFCA Cybersecurity Council will continue on as a permanent group.