CMS Releases New HIPAA Administrative Simplification Fundamentals Fact Sheet. The Centers for Medicare & Medicaid Services' (CMS) National Standards Group (NSG) released its new HIPAA Administrative Simplification Fundamentals Fact Sheet (PDF), located on the HIPAA and Administrative Simplification webpage of the Administrative Simplification website. The new resource provides an overview of Administrative Simplification, its purpose, goals, and how the health care industry benefits from it.

OCR Penalizes Organization for Timely Access Infraction. The Office for Civil Rights (OCR) announced a civil monetary penalty (CMP) of $115,200 collected against a provider of emergency medical services. The CMP was the result of an investigation based on a complaint that the organization had failed to provide a patient with timely access to their medical records. OCR received a complaint alleging that it failed to provide a patient with timely access to their medical records after numerous failed attempts by the patient. OCR initiated an investigation and found that it failed to provide the patient with timely access to their medical records. In response to OCR's investigation, the organization sent the patient a copy of their requested records and amended its internal procedures to streamline and better track right of access requests to follow the law. In October 2023, OCR issued a Notice of Proposed Determination seeking to impose a CMP. OCR finalized its determination and imposed the penalty. View the Notice of Proposed Determination here and the Notice of Final Determination here.

Reminder: 2024 CAQH Index Submission Period Closing Soon. The 2024 CAQH Index submission date is closing soon. All health plans and providers are invited to participate in the survey. The CAQH Index report is leveraged by policy makers and health IT professionals as the industry benchmark for tracking administrative transactions. As a participant you will receive a customized benchmark report that allows you to compare your organization's estimates to national averages. If you are a medical or dental provider, click here to complete the survey. If you are a medical or dental plan, email insights@caqh.org to be sent the survey directly.

HHS 405(d) Moving to ASPR. The Department of Health and Human Services (HHS) announced that the 405(d) Program, a public-private sector security initiative, is transitioning to the Administration for Strategic Preparedness and Response (ASPR) as part of a broader HHS Cybersecurity Strategy for the Healthcare and Public Health Sector. By consolidating efforts within ASPR, HHS seeks to execute HHS' Cybersecurity Strategy through a centralized capability and provide enhanced support to the sector. The transition will ensure that HHS continues the critical 405(d) Program mission with reinforced capabilities, underscoring HHS' commitment to advancing cybersecurity resilience. ASPR's expertise is expected to provide additional technical support, streamline efforts, and unify stakeholder communications to enhance HHS efforts to address critical cybersecurity threats. This transition also leverages ASPR's role and resources as the Sector Risk Management Agency for the sector. Read the press release here.

HC3 Publishes Sector Alert on Phishing Attacks. The Health Sector Cybersecurity Coordination Center (HC3) published a new Sector Alert titled "Phishing Attacks Following Global Technology Outage." This alert is in response to the July 19, 2024 technology outage caused by a defective software update. The outage impacted hospitals, transportation services, financial institutions, media services, and others. The Alert highlights the phishing and other social engineering attacks targeting these and other service industries. Cyber criminals can send messages claiming to work for a cybersecurity firm and offer assistance. This approach can result in data exfiltration, ransomware deployment, and extortion. In its Alert, HC3 details sample counterfeit domains already annotated, the potential impact of the outage to health care organizations, and recommended mitigations from social engineering attacks.

New Executive Director Named at CISA. The Cybersecurity and Infrastructure Security Agency (CISA) named Bridget Bean to replace Brandon Walesa as its executive director. Wales spent three years as executive director with the agency. Bean was formerly the Assistant Director for Integrated Operations. Read the CISA statement here.

Blood Donation Organization Experiences Ransomware Attack. OneBlood, a blood donation organization serving hundreds of hospitals, announced it had experienced a ransomware attack. OneBlood stated it is working closely with cyber security specialists, and federal, state and local agencies as part of its comprehensive response to the situation. The organization remains operational and continues to collect, test and distribute blood, although they are operating at a significantly reduced capacity. To augment their supply, the national blood community is assisting OneBlood by sending blood and platelets to OneBlood.

AHRQ Announces New AI Funding Opportunity. The Agency for Healthcare Research and Quality (AHRQ) published a Notice of Funding Opportunity (NOFO) Examining the Impact of Artificial Intelligence (AI) on Healthcare Safety. The purpose of this NOFO is to invite grant applications that support healthcare safety by determining: (i) whether and how certain breakthrough uses of AI systems can affect patient safety; and (ii) how AI systems can be safely implemented and used. AHRQ notes that AI has the potential to improve the safety, effectiveness, efficiency, accessibility, and affordability of health care. However, AHRQ reminds the industry that these potential improvements must be weighed against potential risks for patient harm and increased user burden. The first application due date is Sept. 25, 2024.