OCR Settles Ransomware Cybersecurity Investigation for $250,000. The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a settlement with a privately-owned health care provider in the state of Washington, concerning potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, following a ransomware attack investigation by OCR. The settlement marks OCR's fourth ransomware settlement as the agency reported a 264% increase in large ransomware breaches since 2018.

OCR initiated an investigation following the receipt of a complaint alleging that provider had experienced a ransomware attack. OCR's investigation determined that approximately 291,000 files that contained electronic PHI (ePHI) were affected. OCR found multiple potential violations of the HIPAA Security Rule, including failures by the provider to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems, and to have sufficient monitoring of its health information systems' activity to protect against a cyber-attack.

Under the terms of the settlement, the provider paid $250,000 to OCR and will implement a corrective action plan that OCR will monitor for two years. These actions include: (i) Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; (ii) Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis; (iii) Developing a written process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; (iv) Developing policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI; (v) Developing written procedures to assign a unique name and/or number for identifying and tracking user identity in its systems that contain ePHI; and (vi) Reviewing and revising, if necessary, written policies and procedures to comply with the HIPAA Privacy and Security Rules. Go here to read the resolution agreement and corrective action plan.

ASTP/ONC Releases Draft Federal FHIR Action Plan. The Assistant Secretary for Technology Policy, Office of the National Coordinator for Health IT (ASTP/ONC) announced the release of the Draft Federal Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) Action Plan. The Plan is a curated catalog of federal agency uses of the HL7 FHIR standard and associated implementation specifications. According to the ASTP/ONC, the draft action plan's goal is to help build an ecosystem for innovation that strengthens consistent agency use of the FHIR standard. The hope is that the FHIR standard's coordinated use across government will help break down the silos separating patients, providers, payers, public health, and research. The Plan focuses on six areas: Core, Network, Payment and Health Quality, Care Delivery and Engagement, Public Health and Emergency Response, and Research. For each area, the agency lists the most mature and broadly applicable FHIR-based implementation specifications including common informative characteristics. ASTP/ONC seeks feedback from agency partners, the standards development community, and subject

matter experts. Comments must be submitted by November 2. Go here to view the Federal FHIR Action Plan.

Feds Issue Warning of China-Sponsored Cyber Attacks. The Federal Bureau of Investigation (FBI), Cyber National Mission Force (CNMF), and National Security Agency (NSA) released a joint advisory warning that the People's Republic of China (PRC)-linked cyber actors have compromised thousands of Internet-connected devices, including small office/home office (SOHO) routers, firewalls, network-attached storage (NAS) and Internet of Things (IoT) devices with the goal of creating a network of compromised nodes (a "botnet") positioned for malicious activity. The actors may then use the botnet as a proxy to conceal their identities while deploying distributed denial of service (DDoS) attacks or compromising targeted U.S. networks.

The FBI recommends network defenders take the following actions to mitigate threats posed by adversaries attempting to use botnets for malicious cyber activity: (i) Disable unused services and ports such as automatic configuration, remote access or file sharing protocols; (ii) Implement network segmentation to ensure IoT devices within a larger network pose known, limited, and tolerable risks; (iii) Monitor for high network traffic volume; (iv) Apply patches and updates, including software and firmware updates; (v) Deploy regular patching; (vi) Replace default passwords with strong passwords; (vii) Plan for device reboots; and (viii) Replace end-of-life equipment with devices that remain in respective vendor support plans.

NIH Awards Grants to Establish a Genomics-Focused National Network. The National Institutes of Health (NIH) announced it was awarding funding worth $27 million over five years to establish the Genomics-enabled Learning Health System Network, which will integrate genomics into learning health systems. The network consists of six clinical study sites and a coordinating center, all of which have an operating learning health system. Each clinical site will propose a project that uses patient data to develop and refine some aspect of genomic medicine. These could include implementing testing for hereditary diseases or using genomic information to select which medications a patient is given. The network also includes a coordinating center, which will select a set of projects that both seem feasible in the program's five-year duration and have the potential to be shared throughout the network.

CMS PY 2023 Cyberattack Reweighting Requests Accepted Until Oct 11. In response to the Change Healthcare cyberattack, the Centers for Medicare & Medicaid Services (CMS) recognized that some clinicians and groups may not have been able to submit a Merit-based Incentive Payment System (MIPS) Extreme and Uncontrollable Circumstances (EUC) Exception Application for performance year (PY) 2023 before the April 15, 2024 deadline. As a result, the agency is permitting clinicians, groups, subgroups, virtual groups, and Alternative Payment Model (APM) Entities to submit a request for reweighting of one or more MIPS performance categories under its EUC exception policies at 42 CFR 414.1380(c)(2) and 42 CFR 414.1317(b)(4) solely on the basis of the Change Healthcare cyberattack, for PY 2023 now through October 11, 2024, at 8 p.m. ET. Applications submitted for reasons outside of the Change

Healthcare cyberattack will be denied. Go here for the 2023 MIPS EUC Reweighting Requests Guide for step-by-step instructions with screenshots.

CMS OMH Announces Six Health Equity Awards. The CMS Office of Minority Health (CMS OMH) announced this year's recipients of funding from the Minority Research Grant Program (MRGP). The six recipients have been awarded grants to advance health equity among the populations served by CMS programs. Each grantee received up to $237,500 in funding to support their projects, totaling $1,423,865 in funding, which will examine critical public health disparities and increase health equity research capacities at minority-serving institutions. The 2024 grantees include:

- **Palo Alto College,** *Palo Alto Dental Hygiene Access to Care Program Enhancing Dental Hygiene Education and Community Health in South San Antonio by Integrating Advanced Sleep Health, CBCT Scans, and Oral Cancer Screening*. Palo Alto College (a Hispanic Serving Institution (HSI)), will offer Cone Beam Computed Tomography (CBCT) scan imaging at a reduced cost to remove financial barriers and improve access to care for at-home sleep study testing. This initiative aims to enhance overall oral health outcomes through early detection and management of conditions related to obstructive sleep apnea identified via clinical and radiographical analysis.

- **Research Foundation CUNY on behalf of Lehman College,** *Studying Substance Use Disorders and Mental Health services in the Bronx using a Health Disparities Research Approach*. The Research Foundation CUNY, an HSI, and the Bronx Community Taskforce will convene with providers across the Bronx to explore factors influencing the utilization of mental health and substance abuse disorder services, including barriers to access and the cultural responsiveness of services, while conducting a rigorous assessment of the services' availability using public Federal, State, and City data. They will analyze the factors that predict their use or underuse by zip code and among populations with higher health burdens of substance abuse and mental health disorders.

- **San Diego State University Foundation,** *Determining Factors Associated with Loss of Independence Among Ethnic Minority Older Adults a 10-year Longitudinal Study Using NHATS Study*. This study by San Diego State, an HSI, aims to identify factors contributing to the loss of independence among multiethnic populations in the U.S. using the WHO's comprehensive multi-dimensional International Classification of Functioning, Disability, and Health (ICF) model, employing a population-based cohort longitudinal design and leveraging the National Health and Aging Trends Study (NHATS) dataset.

- **North Carolina Agricultural and Technical State University,** *Building a Path to Health Equity: Investigating Lead Exposure, Chronic Stress, and Cardiovascular Dysfunction*. North Carolina Agricultural and Technical College, a Historically Black College and University (HBCU) hypothesizes that lead (Pb) exposure, chronic stress, and their interaction contribute to adverse

cardiovascular health outcomes. The main statistical analysis will use model-based methods for cross-sectional clustered data to assess a composite index of cardiovascular dysfunction as the primary outcome. Secondary outcomes include eight cardiovascular measures, isoprostane, and inflammatory biomarkers, accounting for chronic and acute Pb exposure, chronic stress, stress-by-exposure interactions, and participant characteristics.

- **Research Foundation of the State University of New York**, *Expanding Access to Perinatal Healthcare and Supportive Services that Address Social Determinants of Health*. The Research Foundation of the State University of New York, an Asian American Native American Pacific Islander-serving institution (AANAPISI) and HSI, seeks to expand services in communities in Queens, New York to reduce the number of pregnant and/or postpartum individuals who are uninsured or go without needed medical care, to expand access to health care and support for expectant families, and to diversify the lactation field.

- **Fayetteville State University**, *HIV/AIDS Virtual Summer Research Institute for Helping Professionals*. Fayetteville State University, an HBCU, plans to expand its curriculum and training focused on HIV/AIDS education, awareness, and prevention among helping professional students by developing an interdisciplinary two-week virtual summer institute and curriculum. The program will provide students with opportunities for active engagement in reflective learning to enhance their knowledge and perception of HIV/AIDS and its prevention.

For more than two decades, the MRGP has supported researchers at minority-serving institutions through funding to explore and address health care disparities affecting racial and ethnic minority groups, people with disabilities, members of the Lesbian, Gay, Bisexual, Transgender, and Queer (LGBTQ+) community, individuals with limited English proficiency, individuals residing in rural areas, and individuals adversely affected by persistent poverty or inequality. Go here to learn more about the Minority Research Grant Program and to sign up for updates on funding opportunities.

House Subcommittee Holds Hearing on CrowdStrike Outage. The U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled “An Outage Strikes: Assessing the Global Impact of CrowdStrike’s Faulty Software Update.” Members heard from CrowdStrike representatives on the recent computer outage that impacted health care and other sectors. Subcommittee Chair Mark E. Green, MD (R-TN), stated “As the July 19th outage has demonstrated yet again, our networks are increasingly interconnected. While we know that nation-state actors and criminals try to exploit our networks, we would not expect companies to defend themselves from these targeted attacks. However,…we do expect companies to implement the strongest cybersecurity practices possible. Our nation’s security depends on a strong public-private partnership for protecting our networks.” Read the opening statements below and watch the hearing here.

Cybersecurity Legislation Introduced in the Senate. The “Health Infrastructure Security and Accountability Act” has been introduced in the U.S. Senate by Senate Finance Committee Chair Ron Wyden (D-OR) and Senator Mark Warner (D-VA). The bill would require HHS to develop and enforce a set of tough minimum cybersecurity standards for health care providers, health plans, clearinghouses and business associates, including stronger standards for systemically important entities and entities important for national security. The Senators contend that the bill would remove the existing cap on fines under the Health Insurance Portability and Accountability Act, which prevent the regulator from issuing fines large enough to deter large corporations from ignoring cybersecurity standards, and provide funding for hospitals to improve their cybersecurity, particularly low-resource hospitals in rural and urban areas. A one-page summary of the bill can be found here. A section-by-section summary can be found here. The legislative text can be found here.