ENERGY & COMMERCE
CHAIR RODGERS

MEMORANDUM

To: Subcommittee on Health Members and Staff
From: Committee on Energy and Commerce Majority Staff
Re: Health Subcommittee Hearing on April 16, 2024

The Subcommittee on Health will hold a hearing on Tuesday, April 16, 2024, at 10:00 a.m. (ET) in 2123 Rayburn House Office Building. The hearing is entitled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack."

I. Witnesses

- **Mr. Greg Garcia**, Executive Director for Cybersecurity, Healthcare Sector Coordinating Council
- **Mr. Robert Sheldon**, Senior Director of Public Policy and Strategy, CrowdStrike
- **Mr. John Riggi**, National Advisor for Cybersecurity and Risk, American Hospital Association
- **Mr. Scott MacLean**, Board Chair, College of Healthcare Information Management Executives (CHIME)
- **Dr. Adam Bruggeman, MD,** Orthopedic Surgeon, Texas Spine Center

II. Background

HHS & Health Care Cyber Security

The Department of Health and Human Services (HHS) is the Sector Risk Management Agency (SRMA) for the health care and public health sectors. Therefore, HHS is responsible for maintaining America's critical health care infrastructure, which includes coordinating with Cybersecurity and Infrastructure Security Agency (CISA) and other agencies on matters relating to cybersecurity. The Administration for Strategic Preparedness and Response (ASPR), through its Division of Critical Infrastructure Protection (CIP), is responsible for leading and coordinating HHS's cybersecurity efforts and external collaboration. HHS has designated ASPR as the "one-stop shop" cybersecurity support function for the healthcare sector. ASPR is charged with enhancing coordination both within HHS and across the federal government, strengthening partnerships with industry, and improving overall incident response expertise and capabilities.

HHS Office for Civil Rights

The HHS Office for Civil Rights (OCR) is responsible for enforcing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules (45 CFR Part 160 and Subparts A and E of Part 164). A HIPAA covered entity must comply with the requirements within these rules to protect the privacy and security of health information. In the event of a breach of unsecured protected health information (PHI), the HIPAA Breach Notification Rule details the required procedure for notifying affected

individuals, the Secretary of HHS, and in some instances, the media.[1] Covered entities under HIPAA include health care service or supply providers that transmit electronic health information in connection to transactions, health plans, and health care clearing houses. The OCR enforces the HIPAA Rules through civil monetary penalties, and in some cases, criminal penalties are enforced by the U.S. Department of Justice. Common rule violations are impermissible PHI use and disclosure, lack of individuals' access to their PHI, or lack of administrative, technical, or physical PHI safeguards. The rules also specify that any business associates that are contracted with a covered entity must be contractually obligated to comply with HIPPA rules. In addition, a business associate is directly liable under the HIPAA rules and subject to civil and, in certain cases, criminal penalties for making disclosures of protected health information that are not authorized by its contract.

Food and Drug Administration (FDA)

The FDA includes cybersecurity as part of its premarket review of a "cyber device," or a medical device that can connect to the internet.[2] The Protecting And Transforming Cyber Healthcare (PATCH) Act, which passed in the Consolidated Appropriations Act of 2023, codified stricter cybersecurity measures and enforcement tools for a new category of "cyber" medical devices. Now, device manufacturers are expected to adhere to several premarket and post-market controls,[3] in addition to new statutory requirements. For example, manufacturers must submit a software bill of materials (SBOM) to streamline the process of identifying potential vulnerabilities.

Change Healthcare Cyberattack

Change Healthcare, a subsidiary of UnitedHealth Group's Optum division, first disclosed a cyberattack on February 21, 2024. Change Healthcare, which merged with UnitedHealth Group in 2022, handles 15 billion transactions annually, making this breach significant to the entire healthcare sector. Following the breach, it has been reported that a cybercriminal group, ALPHV/Blackcat, was responsible. ALPHV/Blackcat is described by the Department of Justice as a prolific global ransomware group that is Russian based. In December 2023, the Department of Justice announced a disruption campaign against them.[4] There have been reports that UnitedHealth Group paid a ransom of $22 million to ALPHV/Blackcat in order to recover stolen data.[5] UnitedHealth Group has not confirmed whether it has paid a ransom. However, there now

[1] Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction must provide notice to prominent media outlets serving the State or jurisdiction, in addition to notifying affected individuals.
[2] Food and Drug Omnibus Reform Act, or FDORA defines a "cyber" device in full as a device that: includes software validated, installed or authorized by the sponsor of the premarket application as a device or in a device; has the ability to connect to the internet; and contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.
[3] E.g., design controls, complaint handling, corrective action and preventative action, adverse event reporting, and corrections and removals.
[4] U.S. Department of Justice, "Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant", 2023. https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
[5] Satter, R., "Hacker forum post claims UnitedHealth paid $22 mln ransom in bid to recover data", *Reuters*, March 5, 2024. https://www reuters.com/technology/cybersecurity/hacker-forum-post-claims-unitedhealth-paid-22-mln-ransom-bid-recover-data-2024-03-05/

has been a second ransomware group demanding that UnitedHealth Group pay for the stolen data taken during the breach.[6]

Following the disclosure of the cyberattack, Change Healthcare announced they had pulled their impacted systems offline. As of now, it has been reported that Optum, United Healthcare, and UnitedHealth Group systems have not been impacted, only Change Healthcare.

The effects of the cyberattack have rippled across the health care sector, with hospitals, physician groups, and pharmacies all experiencing significant impacts to their operations. Disruption in cash flow, pharmacy services, prior authorization, and claims processing have all been reported. While Change Healthcare has offered workarounds, including switching clearinghouses, many health care entities are concerned about the administrative cost and the timing of the implementation of these suggested solutions.

Administration Response

The Centers for Medicare and Medicaid Services announced accelerated payments to Part A providers, and then subsequently announced Part B advanced payments for providers impacted by the cyberattack. Additionally, ASPR has been leading the health care response in coordination with CISA and the Federal Bureau of Investigation (FBI). The HHS Office of Civil Rights put out a Dear Colleague following the Change Healthcare cyberattack.[7]

Resources:

- Joint Advisory released by the FBI, CISA, and HHS
- HHS Investigation into UHG
- CMS Medicaid flexibilities
- December 2023: HHS Strategy for Health Sector Cybersecurity
- CMS March 9 Statement on Change Healthcare Cyberattack
- HPH Cybersecurity Performance Goals
- CMS fact sheet on payments

III. Staff Contacts

If you have questions regarding this hearing, please contact Emma Schultheis of the Committee staff at 202-225-3641.

[6] Satter, R., "Hackers claim to have UnitedHealth's stolen data - is it a bluff?", *Reuters*, April 9, 2023. https://www reuters.com/technology/hackers-claim-have-unitedhealths-stolen-data-is-it-bluff-2024-04-09/
[7] U.S. Department of Health and Human Services, "Re: Cyberattack on Change Healthcare; Dear Colleagues", 2024. https://www hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf