United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

June 5, 2024

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Ave, S.W.
Washington, D.C. 20201

Dear Secretary Becerra:

I write to urge the Department of Health and Human Services (HHS) to take immediate, enforceable steps to require large healthcare companies to improve their cybersecurity practices. The agency's current approach of allowing the health sector to self-regulate cybersecurity is insufficient and fails to protect personal health information as intended by Congress. HHS must act now to address corporations' lax cybersecurity practices, which have enabled hackers to steal patient health information and shut down parts of the health care system, causing actual harm to patient health.

On May 1st, the Senate Committee on Finance held a hearing to assess the cyberattack against Change Healthcare (a subsidiary of UnitedHealth Group (UHG)), which is the largest health care company in the U.S. During the hearing, Andrew Witty, the chief executive officer of UHG, revealed that hackers gained initial access to the company's network using a compromised username and password to login to a server that was not protected by multi-factor authentication (MFA). The devastating ransomware attack would have been prevented had the company used MFA, a basic cybersecurity defense which federal agencies are required to use, and required of several industries regulated by other agencies.[1] However, HHS does not require health care companies to use MFA, nor does HHS require covered entities or business associates to adopt any other specific cybersecurity best practices.

HHS' failure to regulate the cybersecurity practices of major health care providers like UHG resulted in what the American Hospital Association has described as the worst cyberattack against the healthcare sector in U.S. history.[2] One-third of Americans may have had their

1 Office of Management and Budget, "M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf; Federal Trade Commission, "FTC Safeguards Rule: What Your Business Needs to Know, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

protected information exposed.[3] In addition, the inability to exchange medical records and complete fundamental insurance functions threatened access to medications for millions of patients while pushing many providers to the financial brink.

UHG is not alone in failing to follow cybersecurity best practices resulting in the theft of sensitive patient data. In 2022, health care organizations reported over 600 breaches affecting nearly 42 million Americans.[4] According to the FBI, the health care and public health sector was the most common ransomware target of any critical infrastructure sector in 2023.[5] For 2022, the Office of Civil Rights reported that hacking was the most common cause of a breach, accounting for 74% of the reports received and 77% of the individuals affected.[6] The harms resulting from hacks are not limited to the theft of sensitive patient data. Researchers have found that cyberattacks can result in delays in access to care and impair health care providers' ability to access electronic medical records at the point of care.[7] A recent study found that these events can also result in higher mortality rates for Medicare patients already admitted in a hospital impacted by ransomware.[8]

It is clear that HHS' current approach to healthcare cybersecurity — self-regulation and voluntary best practices — is woefully inadequate and has left the health care system vulnerable to criminals and foreign government hackers. HHS must follow the lead of other federal regulators in mandating cybersecurity best practices necessary to protect the health care sector from further, devastating, easily-preventable cyberattacks. To its credit, HHS announced last year that it planned to update the cybersecurity regulations for the healthcare sector, which HHS has not meaningfully updated since 2003.[9] HHS can and should go further given its role as a

---

2 Letter from the American Hospital Association to Chairman Wyden and Ranking Member Crapo, March 13, 2024, https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack

3 TechCrunch, "UnitedHealthcare CEO says 'maybe a third' of US citizens were affected by recent hack", May 1, 2024, https://techcrunch.com/2024/05/01/united-healthcare-ceo-says-maybe-a-third-of-u-s-citizens-were-affected-by-recent-hack/

4 Department of Health and Human Services, "Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Year 2022," https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf

5 Federal Bureau of Investigation, "Internet Crime Report 2023," https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf

6 Department of Health and Human Services, "Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Year 2022," https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf

7 Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. Health Serv Res. 2019 Oct;54(5):971-980. Available at: 10.1111/1475-6773.13203; Dameff C, Tully J, Chan TC, et al. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Netw Open. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270; https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/

8 McGlave, Claire and Neprash, Hannah and Nikpay, Sayeh, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). Available at SSRN: https://ssrn.com/abstract=4579292

9 https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA22

regulator and purchaser of health coverage for more than 150 million Americans.[10] Specifically, I urge HHS to take the following actions to ensure a robust and resilient healthcare system and to protect patient health information.

First, HHS should require minimum, mandatory technical cybersecurity standards for systemically important entities (SIEs), including clearinghouses and large health systems. These technical standards should address how organizations protect electronic information as well as ensure the health care system's resiliency to these attacks by continuing its critical functions including maintaining access to medical records, providing medical care, and supporting community health.[11] HHS should reinforce these standards and ensure broad adoption by requiring entities that participate in the Medicare program to meet these requirements.

Second, HHS should require SIEs to meet resiliency requirements, so they are able to get back up and running quickly if they are infected with ransomware. SIEs must be capable of rebuilding their information technology infrastructure from scratch and within 48-72 hours. HHS should also stress test these companies to prove they can meet those requirements. It is not acceptable for an SIE like Change Healthcare to be down for more than 6 weeks.

Third, HHS should conduct periodic cybersecurity audits of covered entities and business associates as part of the audits required by Section 13411 of the HITECH Act. The Department has not conducted an audit since 2017, which officials have attributed to a lack of resources.[12] HHS has already indicated through proposed rulemaking that it intends to restart these audits by re-assessing the 207 covered entities and business associates that participated in the agency's prior round of audits. I urge HHS, instead, to prioritize audits of SIEs, even if those organizations were not previously subjected to HHS audits.[13]

Lastly, HHS should provide technical assistance on cybersecurity to health care providers. The Centers for Medicare & Medicaid Services (CMS)'s Quality Improvement Organizations and Medicare Learning Network programs are vital tools at HHS' disposal for improving the effectiveness, efficiency, and quality of health care services delivered to Medicare beneficiaries. HHS should leverage these programs to provide cybersecurity technical assistance and guidance to providers, particularly those with low resources.

---

10 Centers for Medicare and Medicaid Services, "Financial Report FY 2023," https://www.cms.gov/files/document/cms-financial-report-fiscal-year-2023.pdf-0

11 Cybersecurity & Infrastructure Security Agency, "National Critical Functions Set," https://www.cisa.gov/national-critical-functions-set

12 Department of Health and Human Services, "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Year 2022," https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2022.pdf

13 Department of Health and Human Services, "Agency Information Collection Request; 60-Day Public Comment Request," 89 FR 9857, https://www.federalregister.gov/documents/2024/02/12/2024-02737/agency-information-collection-request-60-day-public-comment-request

The current epidemic of successful cyberattacks against the health care sector is a direct result of HHS's failure to appropriately regulate and oversee this industry, harming patients, providers, and our national security. I urge HHS to use all of its authorities to protect U.S. health care providers and patients from cybersecurity risk.

Sincerely,

Ron Wyden
United States Senator
Chairman, Committee on Finance