PHiT
PHARMACY HEALTH
INFORMATION TECHNOLOGY
COLLABORATIVE

Via Electronic Submission to: https://www.regulations.gov

June 3, 2024

Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security
Arlington, VA 22209

Re: [Docket No. CISA-2022-0100] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Dear Mr. Klessman:

On behalf of its membership, the Pharmacy Health Information Technology Collaborative (PHIT) is pleased to submit comments for the proposed rule *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*.

PHIT has been involved with the federal agencies, including the Department of Health and Human Services (HHS) Office of the National Coordinator (ONC) and the Centers for Medicare & Medicaid Services (CMS), in developing the national health information technology (HIT) framework for implementing secure access of electronic health information to improve health outcomes since 2010.

Pharmacists provide essential, patient-centered care services to their patients, including Medicare and Medicaid beneficiaries. Pharmacists use health IT, provider directories, telehealth, e-prescribing (eRx), electronic medical record (EMR)/electronic health record (EHR) systems, and certified EHR technology (CEHRT) to help manage patients' health needs. PHIT supports the use of these systems, which are important to pharmacists in working with other health care providers to deliver longitudinal person-centered care planning, medications used, and transmit patient information related to overall patient care, transitions of care, , medication lists, medication allergies, patient problem lists, smoking status, and social determinants of health (SDOH). Pharmacists also use health IT for reporting to public health agencies (e.g., immunization reporting), clinical decision support services/knowledge artifacts, checking drug formularies checking, and comprehensive medication management (CMM).

Comments

PHIT is supportive of the proposed Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements and the criteria set forth for determining who would be a covered entity for reporting purposes, as outlined in §226.2 (Applicability, page 23767, *Federal Register*). PHIT supports the covered entity determination based on meeting either the small business size standard or the sector-based criteria.

As PHIT understands the proposal, if an entity (e.g., pharmacy) meets one of the two criteria outlined, then the entity is a covered entity under CIRCIA and must report a cyber incident to CISA. The two criteria are: 1) exceeds the small business size standard specified by the North American Industry Classification System Code (NAICS) in the U.S. Small Business Administration (SBA) size regulations, or 2) meets the sector-based criterion. If neither criterion is met, then the entity is not a covered entity and would not be required to report a cyber incident to CISA, though, an entity may need to report a cyber incident to other agencies (e.g., FDA, CMS, ONC, HIPAA, etc.) if required by those agencies, as CIRCIA does not supersede the authority or requirements of other agencies. We also understand this to mean that only the covered entity experiencing a cyber incident would be required to report the incident to CISA. Is our understanding correct? Please clarify for us if it is not.

PHIT also recommends that CISA review the proposed *2024-2030 Federal Health IT Strategic Plan*, if it has not already done so. PHIT strongly believes there should be a coordinated effort among federal agencies to ensure that cybersecurity is a high priority.

Cybercrimes in the United States are increasing at an alarming rate, costing millions of dollars, and show that the U.S. is vulnerable and not adequately prepared to fight them.[1] Targeted victims of cybercrimes include governments (federal,[2] state and local agencies[3]); individuals; businesses, especially health care; etc. Recent attacks, particularly the February ransomware attack on Change Healthcare, the largest health care payment processor in the U.S., disrupted services across the country. "The attack threatened health care workers' paychecks, impacted the ability to fill prescriptions, and even disrupted patient care throughout the health care system."[4] Change Healthcare finally confirmed at a recent U.S. Senate hearing that it paid hackers a $22 million ransom and "that patient data nonetheless ended up on the dark web."[5]

[1] "The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be," U.S. Government Accountability Office (GAO), August 29, 2023. https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be

[2] Sean Lyngaas, "Exclusive: US government agencies hit in global cyberattack," CNN, June 15, 2023. https://www.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html

[3] Sophia Fox-Sowell, "Cyberattacks on state and local governments rose in 2023, says CIS Report," StateScoop, January 30, 2024. https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024/#:~:text=Cybersecurity-,Cyberattacks%20on%20state%20and%20local%20governments%20rose%20in%202023%2C%20says,increased%20in%20frequency%20last%20year

[4] "The U.S. Now Has a National Cybersecurity Strategy, but Is It as Strong as It Could Be?" GAO, March 21, 2024. https://www.gao.gov/blog/u.s.-now-has-national-cybersecurity-strategy-it-strong-it-could-be

[5] Andy Greenberg, "Change Healthcare Finally Admits It Paid Ransomware Hackers $22 million – and Still Faces a Patient Data Leak," *Wired*, April 22, 2024. https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/#:~:text=Updated%2010%3A25%20am%20ET,paid%20%2422%20million%20in%20ransom.

PHIT noted in its May 28, 2024 comments on the Federal Health IT Strategic Plan to the Office of the National Coordinator (ONC) that, as currently drafted, cybersecurity does not come across as a high priority. CISA may be able to offer suggestions for strengthening Goal 4, Objective D of the strategic plan, if it has not already done so.

****

The Pharmacy HIT Collaborative comprises the major national pharmacy associations, representing 250,000 members. PHIT's membership is composed of the key national pharmacy associations involved in health IT, the National Council for Prescription Drug Programs, and 12 associate members encompassing e-prescribing, health information networks, transaction processing networks, pharmacy companies, system vendors, pharmaceutical manufacturers, and other organizations that support pharmacists' services.

As the leading authority in pharmacy health information technology, PHIT's vision and mission are to ensure the U.S. health IT infrastructure better enables pharmacists to optimize person-centered care. Supporting and advancing the use, usability, and interoperability of health IT by pharmacists for person-centered care, PHIT identifies and voices the health IT needs of pharmacists; promotes awareness of functionality and pharmacists' use of health IT; provides resources, guidance, and support for the adoption and implementation of standards-driven health IT; and guides health IT standards development to address pharmacists' needs. For additional information, visit www.pharmacyhit.org.

*****

On behalf of PHIT, thank you again for the opportunity to comment on *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements.*

For more information, contact Shelly Spiro, executive director, Pharmacy HIT Collaborative, at shelly@pharmacyhit.org.

Respectfully submitted,

Shelly Spiro

Shelly Spiro, RPh, FASCP
Executive Director, Pharmacy HIT Collaborative
shelly@pharmacyhit.org

Ilisa BG Bernstein, PharmD, JD, FAPhA
Senior Vice President, Pharmacy Practice &
Government Affairs
American Pharmacists Association (APhA)
IBernstein@aphanet.org

Arnold E. Clayman, PD, FASCP
Vice President, Professional Affairs
American Society of Consultant Pharmacists
aclayman@ascp.com

Scott Anderson, PharmD, MS, CPHIMS,
FASHP, FVSHP
Director, Member Relations
American Society of Health-System Pharmacists
SAnderson@ashp.org

Randy Craven
Project Manager, Medication Therapy
Management (MTMP)
Centene Evolve Pharmacy Solutions Wellcare
randy.craven@wellcare.com

Paul Wilder
Executive Director
CommonWell Health Alliance
paul@commonwellalliance.org

Samm Anderegg, PharmD, MS, BCPS
Chief Executive Officer
DocStation
samm@docstation.com

Youn J. Chu, PharmD, RPh
Clinical Consultant, Pharmacy Transformation
EnlivenHealth an Omnicell Innovation
youn.chu@omnicell.com

Anne Krolikowski, CAE
Executive Director
Hematology/Oncology Pharmacy Association
akrolikowski@hoparx.org

Krystalyn Weaver, PharmD, JD
Executive Vice President & CEO
National Alliance of State Pharmacy
Associations
KWeaver@naspa.us

Ronna B. Hauser, PharmD
Senior Vice President, Policy & Pharmacy Affairs
National Community Pharmacists Association
(NCPA)
ronna.hauser@ncpa.org

Stephen C. Mullenix, BPharm, RPh
Executive Vice President Public Policy &
Professional/Industry Relations
National Council for Prescription Drug Programs
(NCPDP)
smullenix@ncpdp.org

Josh Howland, PharmD, MBA
President Pharmacy Systems
RedSail Technologies, LLC
Josh.Howland@redsailtechnologies.com

Ross E. Pope
CEO
Prescribery
ross@prescribery.com

Paige Clark, RPh
VP of Pharmacy Programs and Policy
Prescryptive
Paige.Clark@prescryptive.com

Jeffery Shick, RPh
Director, Translational Informatics
Digital & Innovation
US Pharmacopeia (USP)
Jeff.shick@USP.org