



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

March 7, 2025

Anthony Archeval, Acting Director
U.S. Department of Human Services
Office for Civil Rights
Attn: HIPAA Security Rule NPRM
Hubert H. Humphrey Building, Room 509F
200 Independence Ave., SW
Washington, DC 20201

Re: [RIN 0945-AA22; Docket ID: HHS-OCR-0945-AA22] HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Acting Director Archeval:

On behalf of its membership, the Pharmacy Health Information Technology Collaborative (PHIT) appreciates the opportunity to submit comments regarding the proposed modifications for *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (ePHI)*.

PHIT has been involved with the federal agencies, including the Department of Health and Human Services (HHS) Assistant Secretary for Technology Policy/Office of the National Coordinator (ASTP/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, who are covered entities under the Health Insurance Portability and Accessibility Act (HIPAA), provide essential, patient-centered care services to their patients, including Medicare and Medicaid beneficiaries, while preserving the security of ePHI. 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, and comprehensive medication management (CMM).

General Comments

PHIT supports updating and modifying HIPAA cyber security standards for protected ePHI and agrees with many of the proposed recommendations; however, we have concerns particularly with a recent development not addressed, which happened after the proposed rule was published.

As covered entities under HIPAA and users of EHR, pharmacists and pharmacy systems protect ePHI and only disclose information that is required for TPO (treatment, payment, and health care operations). Pharmacies, especially independent pharmacies, have not been targets of cyberattacks.

Overview

Cyber security is a major concern that needs to be addressed and protecting ePHI is paramount. The U.S. lags other countries in this area from federal and state governments to the private sector. Health care is the number one target experiencing cyberattacks.¹ The reason for this is health care data is valuable; worth a lot of money to attackers.² Attacks range from stealing personally identifiable information that is sold to black market operators to holding electronic health care systems and organizations hostage via ransomware; UnitedHealth Group paid nearly \$3 billion in ransom in a 2024 attack,³ making it the largest ransom paid to date. This information, including ePHI, is not only being stolen from the private sector but also from the federal government.

Cyberattacks on health care organizations hit an all-time high in 2023.⁴ In 2024, the health care industry experienced its biggest data breaches of all time with attacks on Change Healthcare (UnitedHealthcare Group; largest breach), Kaiser Foundation Health Plan (second biggest), and Ascension Health (third).⁵ The federal government was not immune to health care cyberattacks, as the Centers for Medicare & Medicaid Services (CMS) reported a major, massive breach of protected health information of 3,112,815 individuals in its system

¹ "FBI Report: Health Care the Top Target by Cyber Attackers," Government Technology, June 27, 2024. <https://www.govtech.com/em/safety/fbi-report-health-care-the-top-target-by-cyber-attackers>

² "9 Reasons why healthcare is the biggest target for cyberattacks." Swivel Secure. <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>

³ Marianne Kolbasuk McGee, "Change Healthcare Attack Cost Estimate Reaches Nearly \$2.9B," Bank Info Security, October 16, 2024. <https://www.bankinfosecurity.com/change-healthcare-attack-cost-estimate-reaches-nearly-29b-a-26541>

⁴ Steve Alder, "Healthcare Data Breach Statistics," *The HIPAA Journal*, January 20, 2025. <https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=2021%20was%20a%20bad%20year,stolen%2C%20or%20otherwise%20impermissibly%20disclosed.>

⁵ Steve Alder, "The Biggest Healthcare Data Breaches of 2024," *The HIPAA Journal*, January 7, 2025. <https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/>

(September 2024);⁶ over 940,000 were Medicare beneficiaries.⁷ An earlier CMS data breach occurred in May 2023, affecting 612,000 Medicare beneficiaries.⁸

After reviewing published reports of cyberattacks from the past 15 years, including government reports, the data show the primary targets of cyberattacks are large health care businesses and organizations and the federal government (e.g., hospitals, health insurance companies, health care technology service providers, and CMS) that store and transmit millions of health data pertaining to individuals; cyberattacks are not targeted at smaller health care providers. These large groups accounted for the larger number of cyberattacks that were experienced by 92% of U.S. health care organizations in 2024.⁹ The ransomware attack on Change Healthcare disrupted pharmacies and other health care providers across the country, though no pharmacies were directly attacked. Pharmacies reported having difficulty processing medications orders, doing billings, etc., at that time. Change Healthcare is a technology service provider of health care billing and data systems and a key node in the U.S. health care system.

Comments

Based on recent developments, strengthening security with additional safeguards where cyberattacks are predominantly occurring should be the focus and priority of modifying the rule, rather than proposing numerous modifications that appear to be an attempt for a one size fits all approach for everyone. Capabilities of smaller, health care groups are different than those of the larger groups, as are their needs.

Given recent events, a larger concern is that ePHI transmitted to federal agencies (e.g., CMS, Department of Labor) from pharmacies and other health care providers may no longer be secure, particularly from possible internal breaches. The federal government is a covered entity under HIPAA and is required to follow HIPAA privacy and security standards. If this supposition is not correct, we would appreciate OCR clarifying the government's responsibility in protecting ePHI that it collects, stores, and transmits.

HIPAA covers software that is used to store, transmit, or process protected ePHI. Any covered entity under HIPAA must ensure the software it uses is HIPAA compliant. Open-source software, such as PuTTY, is not inherently HIPAA compliant. It appears PuTTY is being used by one agency.¹⁰ Use of open-source software issue may need to be readdressed in the proposal to protect data provided to the government from health care providers.

⁶ Ibid.

⁷ Esperance Becton & Stephanie Marcantonio, "Over 940,000 Medicare Beneficiaries Impacted by Data Breach," Healthcare Law Blog, October 23, 2024. [https://www.sheppardhealthlaw.com/2024/10/articles/centers-for-medicare-and-medicaid-services-cms/over-940000-medicare-beneficiaries-impacted-by-data-breach/#:~:text=The%20Centers%20for%20Medicare%20%26%20Medicaid,%20and%20personally%20identifiable%20information%20\(%E2%80%9C](https://www.sheppardhealthlaw.com/2024/10/articles/centers-for-medicare-and-medicaid-services-cms/over-940000-medicare-beneficiaries-impacted-by-data-breach/#:~:text=The%20Centers%20for%20Medicare%20%26%20Medicaid,%20and%20personally%20identifiable%20information%20(%E2%80%9C)

⁸ "CMS Responding to Data Breach at Contractor," CMS Newsroom, July 28, 2023. <https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor>

⁹ Steve Alder, "92% of U.S. Healthcare Organizations Experienced a Cyberattack in the Past Year," *The HIPAA Journal*, October 9, 2024. <https://www.hipaajournal.com/92pc-us-healthcare-organizations-cyberattack-past-year/#:~:text=The%20survey%20was%20conducted%20on,88%25%20of%20respondents%20in%202023.>

¹⁰ David Ingram, "DOGE software approval alarms Labor Department employees," NBC News, February 13, 2025. <https://www.nbcnews.com/tech/security/doge-software-approval-alarms-labor-department-employees-data-security-rcna191583>

The federal government experiences cyberattacks frequently. The Office of Management and Budget (OMB) reported that over a 12-month period in fiscal year 2023, federal agencies reported 32,211 information security incidents (up 10% from 2022) and 11 major cyber incidents; the CMS breach was one of the 11 incidents (and another massive breach in 2024).¹¹

OCR should also examine more closely the serious threat of internal breaches within government agencies receiving ePHI; updates to the rule need to account for and cover this, as it is a new evolution since the proposed modifications were published. We would appreciate OCR's thoughts on the aforementioned concerns.

A. Section 160.103—Definitions (3. Proposals: Transmission Media)

As mentioned previously, pharmacies are generally not the target of health care cyberattacks, and they are protecting ePHI. One reason pharmacies are not subject to cyberattacks is related to OCR's proposed revision of "transmission media." Revising the description of "transmission media" to say data are "transmitted almost exclusively by electronic form today" is an unnecessary change and not fully correct. The current description says, "Transmission media used to exchange information already in electronic storage media." The definition then lists examples of various transmission media used.

Large amounts of health data are not transmitted in electronic form. Pharmacies, hospital systems, post-acute care facilities, and many health care providers and insurance payers continue using fax machines, especially for the transmission of prescriptions and other patient information, because they are more secure from data breaches than electronic transmissions.

There are more than 67,000 community pharmacies in the United States; nearly 19,000 of those are independent pharmacies. HIPAA security rule safeguards for fax machines used by pharmacies are followed. "Fax machines remain the most prevalent form of communication for transmitting care records and prescriptions," according to the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC),¹² though progress is slowly being made in moving away from fax machines. Another reason that fax machines continue to be used in health care is the challenges with interoperability between different EHR systems; interoperability is not where it needs to be.

PHIT recommends leaving the transmission media description as is. The proposed change does not clarify anything.

IV. Section-by-Section Description of the Proposed Amendments to the Security Rule

PHIT supports the additions and clarifications of definitions as proposed.

C. Section 164.306 – Security Standards: General Rules

PHIT agrees that much has changed since the final rule was adopted in 2003 and revisions in 2013. In general, the modifications make sense; however, some of the modifications appear to be

¹¹ Shweta Sharma, "11 times the US government got hacked in 2023," CSO Online, June 13, 2024. <https://www.csoonline.com/article/2145769/11-times-the-us-government-got-hacked-in-2023.html>

¹² Lucas Mearian, "The fax is still king in healthcare – and it's not going away anytime soon." *Computerworld*. May 22, 2023. <https://www.computerworld.com/article/1626950/the-fax-is-still-king-in-healthcare-and-its-not-going-away-anytime-soon.html>

adding layers and costs, while removing flexibility that is needed for smaller health care providers who may not have the capabilities or financial resources to implement. Some areas of the cost analysis provided in the proposal appear to be too low.

D. Section 164.308—Administrative Safeguards

Requiring small health care providers to conduct and maintain an accurate and thorough written technology asset inventory, a network map of its electronic information systems, provide a risk analysis, etc., would be overly burdensome and costly. Most small health care providers do not have staff to do this. This would likely require outsourcing to a technology expert, which is not necessarily inexpensive. The more logical approach would be to require the systems developers to provide this type of documents to health care providers using their systems.

E. Section 164.310—Physical Safeguards

PHIT agrees with the proposed modifications. Regarding frequency of reviewing written policies and procedures, that should be done as changes are needed.

F. Section 164.312—Technical Safeguards

PHIT agrees that the proposed modifications are needed, though, the system developer or vendor should work with health care provider to implement. Health care providers, particularly small ones, may not have the technical expertise to implement these.

G. Section 164.314—Organizational Requirements

PHIT supports adding the requirement for a business associate agreement to include a provision for a business associate notify the covered entity activation of its contingency plan in a prompt manner (no more than 24 hours), especially for emergencies (e.g., weather events), for protecting systems and ePHI.

K. New and Emerging Technologies Request for Information (Artificial Intelligence)

“Artificial intelligence [AI] is a double-edged sword that can be used as a security solution or as a weapon by hackers.”¹³ More than ever, cyberattackers are leveraging artificial intelligence to weaponize malware and execute stealth attacks to counter cybersecurity solutions.¹⁴ In reading the discussion provided in the proposed rule and regarding the questions in the request for comment section, the HIPAA security rule is inadequate to address technologies involving ePHI. The advancements and continued evolution of AI is lightyears ahead of the HIPAA. The HIPAA security rule needs to be fully rewritten, not modified, to address concerns with AI and other evolving technologies. As we mentioned earlier, the proposed modifications appear to be just adding layers and costs to covered entities without addressing the actual causes of cyberattacks to gain ePHI and how to thwart them as best as possible, understanding that it will never be 100%.

¹³ Julien Legrand, “Artificial Intelligence as Security Solution and Weaponization by Hackers,” *CISO MAG*, December 19, 2019. https://cisomag.com/hackers-using-ai/#google_vignette

¹⁴ *Ibid.*

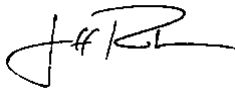
The Pharmacy HIT Collaborative comprises the major national pharmacy associations, representing 250,000 members. PHIT's membership is composed of the key national pharmacy associations involved in health IT, the National Council for Prescription Drug Programs, and 12 associate members encompassing e-prescribing, 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 *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information*.

For more information, contact Jeff Rochon, Executive Director, Pharmacy HIT Collaborative, at jeff@pharmacyhit.org.

Respectfully submitted,



Jeff Rochon, Pharm.D.
Executive Director, Pharmacy HIT Collaborative
jeff@pharmacyhit.org

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

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

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

Michael Baxter, MA
Vice President, Government Affairs
American Pharmacists Association
mbaxter@aphanet.org

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

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

Anne Marie Biernacki
Chief Technology Officer, Co-Founder
ActualMeds Corp.
ambiernacki@actualmeds.com

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

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