hackerone

March 7, 2025

VIA ELECTRONIC SUBMISSION

Re: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

HackerOne Inc. ("HackerOne") submits the following comments in response to the Department of Health and Human Services ("HHS") notice of proposed rulemaking ("NPRM"), "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information."[1] HackerOne appreciates the opportunity to provide input, and we commend the HHS for its openness in working with industry stakeholders on this important issue.

HackerOne is the global leader in human-powered security. We leverage human ingenuity to pinpoint the most critical security flaws across your attack surface to outmatch cybercriminals. HackerOne's Attack Resistance Platform combines the most creative human intelligence with the latest artificial intelligence to reduce threat exposure at all stages of the software development lifecycle. From meeting compliance requirements with pentesting to finding novel and elusive vulnerabilities through bug bounty, HackerOne's elite community of ethical hackers helps organizations transform their businesses with confidence. HackerOne has helped find and fix vulnerabilities for sector leaders including Coinbase, General Motors, GitHub, Goldman Sachs, Hyatt, PayPal, and the U.S Department of Defense.

HackerOne generally supports HHS's desire to update the HIPAA Security Rule to better reflect the modern security best practices needed to combat the increasing cyber threats facing healthcare systems and protect electronic protected health information ("ePHI"). In particular, we appreciate the positive approaches, such as the proposed implementation specification for penetration testing at 45 CFR 164.312(h)(2)(iii).

However, we believe that the NPRM does not adequately take account of the burgeoning and underutilized security researcher community and the security-enabling policies and programs that they provide. HackerOne respectfully recommends modifying the proposed rule to include the following increasingly accepted policies and best practices:

Require a Vulnerability Disclosure Policy (VDP) - Section 164.312(H)(1)-Standard: Vulnerability Management / Section 164.308(A)(5)(I)-Standard Risk Management

[1] U.S. Health and Human Services Department, *Request for Comment on HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information,* 90 Fed. Reg. 898 (Jan. 6, 2025), *available at,* https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

HackerOne appreciates the proposal in the NPRM to add new standards at 164.312(H)(1)-Standard: Vulnerability Management and 164.308(A)(5)(I)-Standard Risk Management to more comprehensively address identifying and managing vulnerabilities. However, HackerOne believes the intent behind these new standards should be further strengthened by adding additional industry accepted and well established best practices. As such, and in line with HHS's request for comment on additional administrative and technical safeguards that the Department should require, we recommend the inclusion of a requirement to implement and maintain a Vulnerability Disclosure Policy ("VDP").

VDPs are centralized processes that allow anyone to report security vulnerabilities in an organization's internet-facing applications. By implementing a VDP, an organization can diversify and enhance the kinds of monitoring processes called for with the NPRM by collecting vulnerability and breach information from previously untapped external sources (e.g., other vendors, service providers, and security researchers).

The benefits of such monitoring processes to HIPAA covered entities are myriad. VDPs encourage individuals to report security risks they encounter, allowing organizations to address these issues promptly before they can be exploited.[2] The formal channels established in VDPs help to ensure disclosed vulnerability information is received by the appropriate team, shortening the length of time between the discovery of the vulnerability and its mitigation. Moreover, since organizations do not need to provide remuneration for vulnerabilities reported to them, VDPs can be a cost-effective tool to meaningfully improve cybersecurity. Incorporating VDPs would not create an undue burden on organizations. As noted in NIST's SP 800-53r5, "vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports." In comparison to other practices, VDPs are not especially complex or resource-intensive. In fact, in a 2020 memo signed by Office of Management and Budget Director Russell Vought, OMB concluded that VDPs "are among the most effective methods for obtaining insights regarding security vulnerability information and provide a high return on investment."[3]

In addition, adding a VDP requirement would support a key goal of the NPRM. Specifically, a VDP would provide public evidence of an entity implementing and deploying policies and processes to manage risks and vulnerabilities.

Numerous organizations in the healthcare sector and beyond already implement VDPs, including the U.S. Department of Health and Human Services (HHS).[4] VDPs are also included

---

[2] HackerOne VDP Report, https://www.hackerone.com/sites/default/files/2021-03/vulnerability-disclosure-policy-what-is-it-why-you-need-one-how-to-get-started.pdf

[3] Office of Management and Budget, Memorandum 20-32, *Improving Vulnerability Identification, Management, and Remediation*, (Sept. 2, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

[4] U.S. Department of Health and Human Services, Vulnerability Disclosure Policy, (Mar. 21, 2023), https://www.hhs.gov/vulnerability-disclosure-policy/index.html

in up-to-date cybersecurity best practices, such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0 (CSF 2.0).[5]

Clarifying the Definition of "Access" – Section 164.304: Definitions

The definition of "access" in the HIPAA Security Rule outlines how users interact with system resources, such as reading, writing, modifying, or using data, which is essential for compliance. However, it does not address the role of good faith security researchers who access systems or data to identify vulnerabilities and improve security without malicious intent. We urge HIPAA to explicitly exclude from the definition of unauthorized access any activities conducted by researchers acting in good faith. This would prevent these activities from being mistakenly treated as violations, allowing covered entities to benefit from researchers' efforts to strengthen the security of ePHI and protect patient data.

Clarifying the Definitions of "Security or Security Measures" and "Security Incident" - Section 164.304: Definitions

The HIPAA Security Rule defines a "security incident" as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations. However, this definition does not account for good faith security research when such activities are not in response to a "specific request" from the covered entity. Many security researchers proactively identify vulnerabilities to improve cybersecurity, even without formal solicitation, and these efforts are critical for maintaining the confidentiality, integrity, and availability of ePHI. We urge HIPAA to explicitly exclude independent, good faith security research from the definition of "security incident," recognizing the value of such work and ensuring it is not penalized. This clarification would foster a stronger cybersecurity ecosystem while protecting the integrity of health information systems.

Clarify the Permissible Use of Bug Bounty Programs (BBPs) - Section 164.312(H)(1)-Standard: Vulnerability Management

HackerOne is pleased to see HHS recognize the value of penetration testing within the NPRM's new standard 164.312(H)(1)-Standard: Vulnerability Management. However, we believe that HHS is missing an opportunity to maximize the benefit of this approach. As such, and in line with HHS's request for comment on whether there are additional implementation specifications that should be adopted for any of the proposed or existing technical safeguards, HackerOne recommends the proposed language for section 164.312(h)(2)(iii) be expanded to clarify that Bug Bounty Programs (BBPs) can be appropriately tailored to comply with, and fulfill, the proposed requirement. Alternatively, we recommend that HHS provide official guidance recognizing that BBPs can be appropriately tailored to comply with the HIPAA Security Rule requirements.

[5] National Institute of Standards and Technology, Cybersecurity Framework 2.0, (Aug. 8, 2023), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Bug Bounty Programs (BBPs) are continuous security tests that offer rewards to ethical security researchers for finding vulnerabilities. In comparison to VDPs, BBPs also allow organizations to seek security information on specific systems, which they can specify in a bounty announcement. BBPs also provide organizations with a broader amount of expertise than traditional penetration testing by tapping into the experience of the global ethical hacker community. BBPs are highly cost-effective in comparison to the cost of responding to a breach or cyber incident, and can be high-impact means of identifying vulnerabilities that may otherwise be overlooked by automated or periodic scanning.

Unfortunately, regulatory ambiguity has contributed to the healthcare industry shying away from this proven method to fortify against cyber threats and adequately protect patient data. Our recommendation would address these concerns and provide additional flexibility to HIPAA covered entities in meeting HIPAA Security Rule requirements.

Clarify the Permissible Use of AI Red Teaming - K. New and Emerging Technologies Request for Information / Section 164.312(H)(1)-Standard: Vulnerability Management

In response to The NPRM section *K. New and Emerging Technologies Request for Information,* and in line with HHS's request for comment on whether there are additional policy or technical tools that the HHS may use to address the security of ePHI in new technologies, HackerOne recommends that HHS explicitly recognize within the HIPAA Security Rule or official guidance that the use of AI Red Teaming activities is permissible and can be appropriately tailored to comply with, and fulfil, either existing HIPAA Security Rule requirements, or those proposed in the NPRM, such as under the penetration testing proposed implementation specification at 164.312(h)(2)(iii).

HackerOne appreciates that the HIPAA Security rule was intended to allow disparate entities flexibility in achieving compliance with requirements even as new technologies emerge. As the healthcare sector becomes increasingly digitized, and as the United States becomes a leader in artificial intelligence (AI) development and implementation, hospitals and other healthcare entities are increasingly making use of AI systems, each of which have a unique set of cybersecurity risks.

One effective way to address these risks is through AI red teaming. AI red teaming is a structured test to find flaws and vulnerabilities in AI systems that could lead to misuse, failure, or unintended consequences. By identifying flaws in AI systems so they can be mitigated before causing harm, AI red teaming is a crucial tool to manage risks to AI security or other unknown outputs. Typically, it takes an adversarial approach, mimicking what could happen if attackers challenged the model's security, performance, and reliability. AI red teaming can evaluate both functional vulnerabilities (e.g., whether security flaws can be exploited) and systemic risks (e.g., how the model might generate harmful outputs).

HIPAA covered entities and business associates would significantly benefit from using AI red teaming to complement the other risk management requirements that exist or that are proposed within the NPRM to better fortify their systems against potential threats.

Modifying HIPAA Security Rule Requirements to Facilitate Additional Security Options

HackerOne strongly recommends that HHS adjust the appropriate elements of the HIPAA Security Rule, including Section 164.308(B) to clarify ambiguity and ease constraints to better allow the healthcare sector to take advantage of the unique benefits the security researcher community can provide. Adjustments may include revising BAA applicability and requirements for good faith security research or creating a new standard within 164.502 covering disclosures by good faith security researchers. Such actions would improve the efficacy of VDPs and incentivize the use of BBPs and AI Red Teaming.

The security researcher community has evolved into a resource for cybersecurity, yet it remains underutilized by the healthcare sector due to misperceptions caused by regulatory ambiguity and unnecessarily restrictive regulations. One key issue is that the current HIPAA framework fails to adequately distinguish between security research conducted in good faith and malicious activity aimed at exploiting data.

Under the existing regulation, even incidental disclosures of ePHI by ethical hackers could be classified as a "breach," necessitating public reporting on the HHS Office of Civil Rights' Breach Portal. This misclassification creates unnecessary complexities that discourage researchers from participating in vulnerability testing, as they are often required to enter into Business Associate Agreements (BAAs) with covered entities. While BAAs serve an important purpose, they impose a range of legal obligations that can act as a barrier to good faith security researchers who solely want to identify and disclose vulnerabilities to protect data from exploitation. HackerOne's proposed recommendation is intended to maximize the permissibility and cost effectiveness of security researcher-enabled security options.

* * *

HackerOne appreciates the opportunity to provide comments on this proposed rule. We look forward to continued engagement with policymakers on these issues and are happy to discuss our response at any time.

Respectfully submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne