hackerone

February 5, 2024

Katherine Ceroalo
New York State Department of Health
Bureau of Program Counsel, Regulatory Affairs Unit
Corning Tower, Empire State Plaza, Rm. 2438
Albany, New York 12237-0031

VIA ELECTRONIC SUBMISSION

Re: New York Hospital Cybersecurity Requirements

Dear Ms. Ceroalo,

HackerOne Inc. (HackerOne) submits the following comments in response to the New York State Department of Health's proposed addition of Section 405.46 to Title 10 of the New York Codes, Rules and Regulations (NYCRR), or the "Hospital Cybersecurity Requirements."[1] HackerOne appreciates the opportunity to provide input, and we commend the New York State Department of Health 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.

While HackerOne broadly supports the New York State Department of Health's efforts to improve cybersecurity in the healthcare sector, we believe that the below key changes would enhance its overall effectiveness.

1. Strengthen Cybersecurity Program Requirements

[1] New York Department of Health, Hospital Cybersecurity Requirements, Dec. 6, 2023, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Hospital%20Cybersecurity%20Requirements.pdf.

In the proposed rule, the New York State Department of Health requires hospitals to have cybersecurity programs that "include monitoring and testing developed in accordance with the hospital's risk assessment."[2] This monitoring must include *at least* annual penetrating testing and automated scans and reviews of IT systems. While these requirements oblige hospitals to assess cybersecurity risks *periodically*, they do not facilitate *continuous* and proactive monitoring, evaluation, and mitigation efforts. Moreover, this language implicitly encourages hospitals to collect and analyze vulnerability information from internal sources (i.e. their own CSIRTs and IT teams) and from organizations with whom the hospital has a contractual relationship (i.e., third party cybersecurity companies). While these sources provide valuable information that will surely improve hospital cybersecurity, vulnerabilities are frequently identified and disclosed by external sources.

To ensure that hospitals receive and respond to vulnerability information from all available sources, HackerOne recommends that the Department of Health add language to Section 405.46 to Title 10 that includes following key cybersecurity safeguards:

a. *Vulnerability Disclosure Programs*

Vulnerability Disclosure Programs (VDPs) are centralized processes that allow anyone to report security flaws in an organization's internet-facing applications. By implementing a VDP, an organization can enhance its traditional monitoring processes by collecting vulnerability and breach information from previously untapped external sources (e.g., other vendors, service providers, and security researchers). The formal channels established in a VDP 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.

Numerous organizations in the healthcare sector and beyond already implement VDPs, including the U.S. Department of Health and Human Services (HHS)[3] and the City of New York.[4] VDPs are also included 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] By adding a VDP requirement to Section 405.46 to Title 10, New York State will ensure that all of its hospitals adopt these same valuable practices to keep systems secure.

b. *Bug Bounty Programs*

[2] New York Department of Health, Hospital Cybersecurity Requirements, Dec. 6, 2023, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Hospital%20Cybersecurity%20Requirements.pdf.

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

[4] City of New York, Office of Technology and Innovation, Vulnerability Disclosure Program, https://nyc.responsibledisclosure.com/hc/en-us (last accessed Jan. 6, 2024).

[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.

c. *AI Red Teaming*

AI Red Teaming is the practice of testing Artificial Intelligence (AI) systems for alignment with security, safety, trustworthiness, and fairness. As the healthcare sector becomes increasingly digitized, hospitals and other healthcare entities are increasingly making use of AI systems, each of which have a unique set of cybersecurity risks. New York's hospitals can use AI Red Teaming to complement their other risk management efforts and fortify their systems against potential threats. Adding a requirement into would also bring Section 405.46 of Title 10 in line with cutting-edge US federal guidance on AI, such as the recent *Executive Order (EO) on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.[6]

Short of adding additional requirements, the New York State Department of Health may also consider simply recommending that hospitals implement VDPs, BBPs, and AI-red teaming as a part of their cybersecurity programs. Then, as hospital cybersecurity programs become more developed, the Department of Health could eventually consider requiring these practices.

2. Lengthen Incident Reporting Timelines

In the proposed rule, the New York State Department of Health requires hospitals to report cyber incidents within two hours.[7] Implementing such a short timeline could harm the overall cybersecurity posture of New York's healthcare sector by interfering with incident response and undermining the quality of incident reporting. In the two hours following an incident, cybersecurity incident response teams (CSIRT) often lack crucial information. If they are forced to report an incident before they fully understand it, there is a risk that the report will include incomplete or inaccurate information that will need to be revised later. To address this issue, HackerOne urges the New York State Department of Health to implement a 72-hour reporting timeframe. This longer timeline would provide the appropriate balance between

[6] White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Oct. 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[7] New York Department of Health, Hospital Cybersecurity Requirements, Dec. 6, 2023, https://regs.health.ny.gov/sites/default/files/proposed-regulations/Hospital%20Cybersecurity%20Requirements.pdf.

urgency and accuracy, ensuring that incident reports are both meaningful and actionable for all stakeholders.

Implementing a 72-hour timeline would also better align Section 405.46 with other established incident reporting timelines. For example, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) has a 72 hour timeline;[8] the EU's General Data Protection Regulation (GDPR) has a 72 hour timeline;[9] and the SEC's Guidance on Public Company Cybersecurity Disclosures has a 4 business-day timeline.[10]

HackerOne also recommends that the New York State Department of Health make the incident reporting provision effective at least one year after the regulation enters into force. This will help ensure that all hospitals and covered entities have sufficient time to develop internal processes and allocate resources for compliance.

Conclusion

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

[8] 6 U.S. Code § 681b, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section681&num=0&edition=prelim

[9] European Union (EU), General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 33.

[10] Securities and Exchange Commission (SEC), Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Jul. 26, 2023, https://www.sec.gov/files/rules/final/2023/33-11216.pdf