HIPAA SECURITY RULE TO STRENGTHEN THE CYBERSECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION

March 7, 2025

I. INTRODUCTION

In response to the Department of Health and Human Services's ("HHS") notice of proposed rulemaking to update the security requirements in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Update") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike supports the HIPAA Update's goal of better protecting hospitals, citizens, and electronic protected health information ("ePHI") from cybersecurity threats. As the HHS knows, healthcare is unfortunately one of the most heavily-targeted critical infrastructure sectors. Cyber threat actors attempt to breach healthcare entities for a variety of reasons based on their different motivations. Cyber criminal (eCrime) actors seek to monetize hacking these entities through ransomware, data extortion, Business Email Compromise (BEC), theft of medical records, and access to banking and payment information. Nation-state actors target the sector seeking information about specific individuals or broad populations for espionage purposes, and could leverage disruptive or destructive attacks to advance geopolitical aims. "Hacktivist" actors may also target entities in the sector, directly or inadvertently, to advance a social or political advocacy agenda.[1]

[1] "*Examining Health Sector Cybersecurity*," CrowdStrike Testimony, April 16, 2024. https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/evo-media-document/Robert%20Sheldon_Witness%20Testimony_04.16.2024.pdf.

These threats continue to evolve and grow more severe. CrowdStrike's latest Global Threat Report notes that interactive intrusion activity against the healthcare sector continues to be significant, with 9% of tracked intrusions targeting the sector in 2024.[2] Additionally, in 2024, China-nexus activity surged 150% and common eCrime technique "Vishing" attacks skyrocketed 442% between the first and second half of 2024 across all sectors – making steps to enhance cybersecurity in the sector timely and appropriate.

While we do not have feedback on every aspect of this proposed regulation, we do want to offer several points that may be of value to the HHS as it considers the proposed regulation.

A. Cybersecurity Risk Management Practices

We commend the HHS for recognizing the changed environment for healthcare and the need to strengthen cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture that would help accomplish the proposed regulation's directive of building a cybersecurity program that identifies and addresses threats. The proposed regulation includes, and is considering, some of today's most effective cybersecurity practices. We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

Organizations should leverage several key technologies to defend against cyber threat actors:

- **Cloud Security**. Leveraging cloud systems provides numerous operational efficiencies and security enhancements. Given today's rapidly evolving threat landscape, organizations must address cloud-specific and cross-domain threats (where adversaries traverse cloud and on-premise environments). Security teams must protect data, manage identity and access, and hunt for and respond to threats in real-time. Capabilities of particular relevance include cloud workload protection, cloud-native application protection platform (CNAPP),

[2] An interactive intrusion occurs when threat actors perform hands-on-keyboard activities within a victim's environment; as opposed to a bot or spam. Interactive intrusions, or hands-on-keyboard attacks, are typically more sophisticated and difficult to detect compared to automated attacks, requiring advanced threat hunting and incident response capabilities to identify and mitigate.
"2025 *Global Threat Report*," CrowdStrike,
https://www.crowdstrike.com/en-us/global-threat-report/.

cloud security posture management (CSPM), and Software-as-a-Service (SaaS) security.

- **Endpoint Detection and Response (EDR)**: EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs, and would be a reasonable area to emphasize in the forthcoming HIPAA Update.

- **Next-Generation Security Information and Event Management (SIEM) solutions.** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by EDR tools) and integrate it with other security-relevant event information from an array of sources. Supported by AI, this provides defenders a more coherent view, intuitive workflows, and ultimately better control of their environments. Given that the entities in scope protect sensitive data, Next-Gen SIEM solutions would be a key addition to the HIPAA Update.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **Identity Threat Detection and Response (ITDR)**: As organizations increase deployment of cloud services, work from anywhere models, and Bring-Your-Own-Device policies, enterprise boundaries continue to erode. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. In fact, compromised valid identities are a common initial access vector in incidents. However, emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should consistently measure and reduce their response time.

- **Threat Hunting**. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year.

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. The HIPAA Update has MFA requirements to further protect entities from identity and credential theft attacks. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Security Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally, or lack the scale to support a robust, 24/7, 365 days per year security capability. Increasingly, such entities should rely upon managed service providers, which can be more efficient overall and enable organizations to apply internal IT/security resources toward domain-specific challenges, including governance, risk, and compliance. Adopting an MSSP can radically strengthen organizations' security posture.

B. Resilient by Design

The HIPAA Update creates new requirements for contingency plans and accurately notes the important relationship between contingency planning and resiliency of a regulated entity's security systems. Following CrowdStrike's faulty content configuration update in July 2024, we identified enhanced testing and resilience actions to help ensure such an event will not happen again.[3] CrowdStrike understands the gravity and impact of the situation, and we have implemented enhanced processes to emphasize resilience across the platform. CrowdStrike will continue to engage with the cybersecurity and IT community to develop best practices for these issues, so the industry as a whole can incorporate lessons learned.

To this end, CrowdStrike developed "Resilient by Design," a framework designed to ensure we can continue accomplishing our mission of stopping breaches and furthering our work to make sure every connected system is as robust as possible.[4] Resilient by Design is both a business framework and a mindset, and it requires commitment and resolve to succeed. It's how we drive resilience across our ecosystem, while also helping our customers become more resilient. This focus enhances our commitment to protect our customers against disruptive cyberattacks, as we have for over a decade.

CrowdStrike is internalizing these pillars. By focusing on Resilient by Design, we can create an ecosystem where these pillars support each other and become a virtuous

[3] "*External Technical Root Cause Analysis*," CrowdStrike, August 6, 2024. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

[4] "*Recognizing the Resilience of the CrowdStrike Community*," George Kurtz, September 25, 2024. https://www.crowdstrike.com/en-us/blog/george-kurtz-resilient-by-design-fal-con-2024/.

cycle.

1. *Foundational*: Resilience must be a foundational element of our company. Everything we do at CrowdStrike will have a lens on how we can enhance resilience. CrowdStrike has detailed many of our process improvements, and we continue in our commitment to strengthen every aspect of what we do, from code and deployment to configuration and support.

2. *Adaptive*: Every entity is different, and as a cybersecurity provider, we need to recognize that one size doesn’t fit all customers. Sectors such as finance, manufacturing, healthcare, utilities, technology, and government have unique, differing needs to deploy a successful cybersecurity program. By addressing this diversity, we can build and deliver highly resilient security solutions and outcomes that fit the needs of our customers.

3. *Continuous*: A perpetual feedback loop–that includes sources such as users, other organizations, and cybersecurity industry stakeholders–enables constant learning and improvement. This continuous learning is already part of CrowdStrike’s DNA; we leverage the power of the cloud and the crowd in the Falcon platform. We also are constantly monitoring what's in the environment, observing threats as they evolve, understanding the adversary's tactics and techniques, learning from and adapting to their tradecraft.

As the HHS understands, pursuing resilience is not optional — it’s essential for all cybersecurity stakeholders. Resilient by Design will drive the next phase of growth for CrowdStrike, the cybersecurity industry, and the broader ecosystem on which we all depend.

C. Definition Harmonization

As the HIPAA Update notes, there are numerous laws and regulations that apply to entities that are also under the scope of HIPAA. However, the HHS has not drawn from an existing “security incident” definition in the updated text, or noted alignment with forthcoming federal definitions, but rather has created a new definition. As the HHS reviews this HIPAA Update, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing rules and regulations. The proposed regulation has the opportunity to strengthen cybersecurity for organizations that play critical roles in the everyday lives of many citizens. Nonetheless, the new regulation will not be issued in a vacuum, but within a variety of cybersecurity regulations. We recommend the Department align future drafts with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") cybersecurity incident definition, and its forthcoming implementing regulation.

Additionally, CrowdStrike recommends amending the "attempted unauthorized access" threshold of the security incident definition to something impact-based. There are significant distinctions between cybersecurity events and incidents, and reporting of issues mitigated or resolved at the event-level is unlikely to provide additional value.

Finally, the HIPAA Update adds several bespoke definitions for common information technology terms. Again, rather than creating new definitions, we encourage HHS to review the National Institute of Standards and Technology's ("NIST") glossary and use their definitions where applicable.

D. Artificial Intelligence

The HIPAA Update describes the benefits Artificial Intelligence ("AI") can bring to the healthcare sector such as improving patient care and reducing costs. As in the healthcare sector, AI can help improve cybersecurity functions. The use of AI to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks, because AI can defeat novel threats based on behavior cues rather than known signatures. Though the HIPAA Update correctly identifies threats to AI systems as a risk, leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats.

III. CONCLUSION

The HHS's HIPAA Update represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the healthcare sector uses strong cybersecurity practices due to the amount of sensitive data they protect and the regulations to which they are subject. With an emphasis on adoption of practical security practices, these new requirements can raise the already high standard of cybersecurity in the healthcare sector. As the HHS moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***