Encryption That Starts Too Late Leaves Healthcare Exposed

Why End-to-End Encryption Must Begin at the Keystroke

Written by Dr. Diane M. Janosek

Dr. Diane M. Janosek, Esq., PhD, brings over 25 years of leadership in national security and cybersecurity, including senior roles at the National Security Agency (NSA) and direct reporting to The White House and the Pentagon.

Dr. Janosek's analysis below independently validates the need for keystroke encryption in healthcare, and as HIPAA already requires protection at creation, keystroke encryption is simply the modern way to meet that requirement.

As federal lawmakers and regulators continue strengthening cybersecurity protections across the healthcare sector, recent initiatives—including The Healthcare Cybersecurity Resilience Act of 2025—underscore a shared priority: safeguarding electronic protected health information (ePHI) against increasingly sophisticated cyber threats. While both HIPAA and its implementing regulations are intentionally technology-neutral, their spirit and legislative intent are equally clear—healthcare cybersecurity requirements must evolve as threats change and as effective security technologies become available.

Implementation historically emphasizes encryption of ePHI at rest and in transit, yet modern attack methods increasingly exploit a critical and under-protected phase of the data lifecycle: the point of creation. Highly sensitive information, such as patient records, usernames, and passwords, can be compromised **before** those protections take effect. Unencrypted keystrokes can be intercepted by keylogging malware, allowing attackers to capture data directly from the keyboard and bypass traditional encryption controls. Keylogging attacks have already impacted major healthcare organizations. Industry data underscores this trend: nearly half of malware detected in 2023 involved keyloggers, and by early 2024, approximately 60% of phishing attacks incorporated keylogging techniques.

The Unaddressed Point of Entry Vulnerability: Encryption Must Protect Data at the Point of Entry (**Create** and Receive)[1]

Under the HIPAA Security Rule, covered entities and business associates are required to protect ePHI they **create**, receive, maintain, or transmit.[2] Despite this lifecycle-based mandate, most healthcare security programs focus on protecting data only after it has been entered into a system. At the moment clinicians or staff type patient information, credentials, or authentication codes via the keyboard of a computer or mobile device, the data exists briefly in plaintext—outside the protection of traditional encryption controls.

[1] U. S. Department of Health and Human Services regulation at 45 C.F.R. Section 164.306(a)(1) refers to create, receive, maintain and transmit. For purposes of this analysis, *point of entry encompasses both creating and receiving* electronic protected health information (ePHI).

[2] *The HIPAA Journal*, Dec. 30, 2024. https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/

This exposure is not hypothetical. Keystroke-logging attacks exploit this precise gap, capturing data at the point of entry and bypassing encryption altogether. A reported 2025 insider-threat case involving the **University of Maryland Medical System**[3] illustrates the real-world consequences of this vulnerability, where a trusted employee used keystroke-logging tools to capture credentials and sensitive information. The incident underscores that keystroke interception is not solely an external threat but a material insider risk in complex healthcare and research environments.

Healthcare was the most targeted critical infrastructure sector in both 2023 and 2024. Ransomware has escalated within the healthcare sector significantly, as well as exploitations of medical applications. In 2024 and 2025, the Chinese threat actor Silver Fox deployed ***ValleyRAT*****,** a backdoor remote access tool (RAT), to gain control of victim computers and to infect them with a keylogger and a crypto miner. Silver Fox's malware masqueraded as legitimate software.[4] The accelerating frequency and complexity of cyber-attacks targeting the healthcare sector, and in turn American patients, is concerning and warrants updated safeguards.

MFA and Traditional Encryption Are No Longer Sufficient Alone: Keystroke encryption strengthens Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is an essential security control, but it depends on the integrity of the device and the credentials being entered. If a keylogger is present, attackers can capture usernames and passwords as they are typed. If that attacker has already compromised a second factor, such as the user's email account, he or she can also intercept one-time passcodes or verification links. In such cases, attackers can defeat MFA without breaching encrypted databases or network transmissions, and this illicit access can go undetected for years.

Keystroke encryption directly addresses the need for updated safeguards by encrypting data at the moment it is created, before it is accessed by the operating system or intercepted by malicious software. Even if keystrokes are captured, they are rendered unreadable and unusable. This capability materially strengthens identity and access management controls and prevents attackers from bypassing MFA through credential and code interception.

Aligning Existing Law with Modern Capabilities

Importantly, adopting keystroke encryption does not require new statutory authority. The HIPAA statute and Security Rule already mandate protection of ePHI across its full lifecycle, **including at creation.** The framework is intentionally technology-neutral, allowing regulated entities to adopt reasonable and appropriate safeguards as technology evolves.[5]

---

[3] At the University of Maryland Medical System and University of Maryland Medical Center (UMMC), a clinical pharmacy specialist used keyloggers to spy on coworkers for a decade. He targeted individuals, most young female pharmacists, residents, and other medical professionals. He used stolen credentials to access webcams and the home security cameras of his victims. Keystroke encryption would have prevented this illicit access. https://www.hipaajournal.com/lawsuit-teaching-hospital-pharmacist-cyber-spying-campaign/

[4] Forescout Research Report (Feb 24, 2025). https://www.forescout.com/blog/healthcare-malware-hunt-part-1-silver-fox-apt-targets-philips-dicom-viewers/

[5] The HIPAA Security Rule requires covered entities and business associates to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" (45 C.F.R. § 164.306(a)(1)). This lifecycle-based obligation requires protection at

Protecting data at the point of **creation** is no longer aspirational—it is achievable through the application of patented and commercially available keystroke encryption technology. Recognizing keystroke encryption as a reasonable and appropriate method to ensure confidentiality, integrity and availability of ePHI would not impose a new legal obligation, but rather clarify how regulated entities may satisfy an obligation that already exists in 45 C.F.R. Section 164.306(a)(1).

Closing the Lifecycle Gap in Healthcare Cybersecurity

Encrypting data at the point of entry closes a critical gap that undermines access controls, identity verification, and traditional encryption strategies. This protection is especially important in healthcare environments characterized by shared workstations, legacy systems, time-sensitive clinical workflows, and extensive third-party integrations.

Explicit regulatory recognition of keystroke encryption would strengthen healthcare cybersecurity resilience, reduce insider-threat risk, and better protect patient privacy—while preserving HIPAA's flexible, technology-neutral framework.

Conclusion: Securing Healthcare Data from the First Keystroke

Protecting ePHI today requires more than securing databases and networks; it requires securing how data initially enters the system. **HIPAA already requires protection at creation.** Now that effective technology exists to meet that requirement, it is reasonable—and expected—for healthcare organizations to adopt it. **Keystroke encryption is not a departure from existing law. It is the modern means of fulfilling it.**

The Health Care Cybersecurity and Resiliency Act of 2025 represents meaningful progress toward stronger healthcare cybersecurity standards. While not necessary by statutory change, policymakers and regulators should explicitly recognize keystroke encryption as a required safeguard to strengthen healthcare defenses against evolving cyber threats and improve patient trust.

***HIPAA already requires protection at creation**, keystroke encryption is simply the modern way to meet that requirement.*
Dr. Janosek, January 2026

(SEE TABLE 1 ON PAGE 4)

the moment ePHI is created, not solely after storage or transmission. Because the Security Rule is intentionally technology-neutral, it permits and anticipates the adoption of reasonable and appropriate technical safeguards as they become available. Where encryption technologies exist that can protect ePHI at the point of creation—such as encrypting data at the moment of keyboard entry—the use of such controls aligns with both the text and intent of the regulation and supports compliance with HIPAA's administrative, physical, and technical safeguard requirements. See HIPAA Table 1.

HIPAA Table 1

HIPAA Requirement	Regulatory Citation	Existing Obligation	How Keystroke Encryption Satisfies It
General Security Standards	45 C.F.R. § 164.306(a)(1)	Protect ePHI that is created, received, maintained, or transmitted	Encrypts ePHI at the moment it is created (keyboard entry), closing a known lifecycle gap
Risk Management	45 C.F.R. § 164.308(a)(1)(ii)(B)	Implement measures to reduce risks identified in risk analysis	Mitigates documented risk of keystroke logging and credential interception
Access Control	45 C.F.R. § 164.312(a)	Protect access to ePHI through technical controls	Prevents compromise of credentials used to access systems containing ePHI
Integrity Controls	45 C.F.R. § 164.312(c)(1)	Protect ePHI from improper alteration or destruction	Prevents unauthorized manipulation enabled by stolen credentials
Transmission Security	45 C.F.R. § 164.312(e)	Protect ePHI transmitted over electronic networks	Secures data before transmission begins by encrypting it at entry
Person or Entity Authentication	45 C.F.R. § 164.312(d)	Verify identity of persons accessing ePHI	Strengthens authentication by preventing interception of login credentials and MFA inputs