HITRUST

6175 Main Street
Suite 400
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

# HITRUST Statement on HIPAA Notice of Proposed Rulemaking

## Overview

The U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) on December 27, 2024, to update the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The NPRM aims to modernize the HIPAA Security Rule published over 20 years ago[1] to address the increasing cybersecurity threats and data breaches in the healthcare sector.

## HITRUST Input to the New Administration and Lawmakers

HITRUST previously provided input[2] to the incoming administration and lawmakers on December 9, 2024, in anticipation of changes to the HIPAA Security Rule. Our letter emphasized the need for meaningful reforms to enhance cybersecurity in the healthcare sector and advocated for leveraging proven, scalable models that enhance security outcomes while avoiding inefficiencies or unnecessary complexity. We based this letter and our input on 17 years of experience, a significantly lower level of observed breaches across HITRUST certified entities, and the overall effectiveness of comprehensive risk management strategies refined over tens of thousands of security assessments in support of healthcare and supporting entities.

## Principal Challenges

Our letter highlighted two principal challenges as well as a series of specific recommendations:

1. **Concerns with Current Regulations**: HITRUST expressed concerns that current regulatory efforts have introduced requirements that are not effective in addressing cybersecurity risks in the healthcare industry.

[1] See https://www.hhs.gov/hipaa/for-professionals/security/index.html.
[2] HITRUST Letter to Robert F. Kennedy, Jr. December 9, 2024. See https://hitrustalliance.net/hubfs/Letters/HITRUST%20Letter%20to%20DHHS%20and%20Committees.pdf.

2. **Need for Clear and Prescriptive Guidelines**: The letter stressed the importance of having relevant, clear, and prescriptive guidelines for controls and assurance to ensure consistent implementation and objective measurement of cybersecurity practices.

**Compliance for HITRUST Certified Entities for the NPRM**

HITRUST and HITRUST certified environments are well positioned against the NPRM requirements. Well over 90% of the requirements of the NPRM requirements are already supported through the HITRUST CSF.[3] Security, risk management, and governance leaders at entities using HITRUST already demonstrate a commitment to mitigating present day risks through measuring and documenting their security maturity and by staying ahead of current and emerging threats while also meeting compliance obligations where the HIPAA Security Rule is tailored into the scope of a HITRUST assessment. HITRUST remains committed to ensuring that highly reliable assurances over controls relevant to today's threats are already present, are regularly updated,[4] and are being implemented by HITRUST Certified Entities.

Most importantly, companies with a HITRUST Certification consistently demonstrate a high level of security effectiveness as demonstrated by the 2024 Trust Report[5] where only 0.64% of HITRUST-certified environments reported breaches in 2022 and 2023. HITRUST sees improved performance in the past year with the percentage of entities reporting breaches further reduced with updated metrics soon to be published in the 2025 HITRUST Trust Report.

An important consideration highlighted by the NPRM and already addressed by the majority of HITRUST customers and relying parties is third party risk management – in this case identified as further obligations by business associates, contractors and now health plan sponsors including new compliance specifications in the NPRM. HITRUST has a long tradition of supporting the oversight obligations that companies implement for the many constituencies in the healthcare industry including initiatives such as the Health Third Party Trust Initiative,[6] integration capabilities such as the HITRUST Assessment XChange[7] and recent integration

[3] HITRUST CSF Version 11.4. See https://hitrustalliance.net/hitrust-framework.
[4] HITRUST Cyber Threat Adaptive. See https://hitrustalliance.net/press-releases/hitrust-enhances-cyber-threat-adaptive-engine-using-microsoft.
[5] HITRUST 2024 *Trust Report*. See https://hitrustalliance.net/trust-report.
[6] Health Third Party Trust Initiative (Health3PT). See https://health3pt.org.
[7] HITRUST Assessment Xchange. See https://hitrustalliance.net/hitrust-assessment-xchange.

with ServiceNow,[8] and tools that facilitate electronic distribution of assurance results.[9] New security and compliance obligations under the NPRM will only be achievable where they are practically implemented and supported across the complex ecosystem of relationships in the healthcare industry.

There are both practical and new challenges that the healthcare industry faces which must be considered by this NPRM. On a practical front, these include support for small and rural health providers which is identified by HHS as a challenge but is not practically achievable with the NPRM as written. HITRUST has proven over the years that security and compliance for the diversity of the healthcare system is only possible through practical engagement of service providers, such as cloud service providers, and shared delivery of security requirements – any future rule must provide a scalable and accessible approach for those entities including the opportunity to inherit security capabilities and assurances from those suppliers.[10] With regard to new risks, the complexity and inherent risk of the use of Generative AI in healthcare is absent from the NPRM. The exciting potential and significant inherent risk of Generative AI in healthcare must be considered in a practical manner that ensures that cyber security threats are identified, understood and addressed. This gap must be closed for any new rule implemented for the current technology landscape and HITRUST provides a pathway to address this growing inherent risk to ePHI for companies that are leveraging Generative AI.[11]

HITRUST customers and healthcare entities can remain confident that changes or new rulemaking under HIPAA framed by the NPRM are practical, achievable and measurable with HITRUST. As noted, we already meet the vast majority of requirements and are committing to provide ongoing and regular analysis to the healthcare market, business associates and contractors as the Notice of Rulemaking moves through the rulemaking process. Without regard to these potential new compliance obligations, HITRUST invites all companies to join with us in implementing relevant security controls that continue to demonstrate risk

[8] HITRUST Assessment XChange for ServiceNow Private Preview. See https://info.hitrustalliance.net/preview.
[9] HITRUST Results Distribution System (RDS). See https://hitrustalliance.net/results-distribution-system.
[10] HITRUST Shared Responsibility and Inheritance Program. See https://hitrustalliance.net/shared-responsibility-and-inheritance-program.
[11]HITRUST AI Security Assessment. See https://hitrustalliance.net/assessments-and-certifications/aisecurityassessment.

management outcomes for themselves and their third-party suppliers including regulated entities such as business associates their contractors and other suppliers.

There are a number of changes that will make the NPRM better and more relevant to the needs of the healthcare industry and HITRUST looks forward to submitting public comments to help guide the direction of the rule. Unless HHS considers the relevance of controls and assurance in the NPRM, the healthcare industry and our nation will invest billions of dollars to comply with this new rule without measurably reducing present day risks to acceptable levels in terms of exposure of and impact to the entire healthcare system. As stated in our letter to the new administration and lawmakers, the risk to our nation if we get this wrong includes requirements that are "not implemented; are not consistently implemented; and/or are not capable of being objectively measured because they are unclear, lack prescription, and are not supported by illustrative procedures that provide clarity of their appropriate implementation, e.g., through the successful implementation of sustaining policies, procedures, and provable implementation outcomes".[12] We look forward to engaging in support of industry companies seeking to meet new requirements, providing assurances to regulators, including the Office for Civil Rights and other healthcare industry companies, and supporting ongoing compliance obligations as we have done for 17 years.

[12] HITRUST "Letter to Robert F. Kennedy, Jr." 4.