

December 9, 2024

VIA Hand Delivery and Email

Robert F. Kennedy, Jr.

Nominee
Secretary of Health and Human Services

House Energy & Commerce Committee

**House Oversight & Accountability
Committee**

House Veteran Affairs Committee

House Ways & Means Committee

House Budget Committee

Senate Appropriations Committee

Senate Budget Committee

Senate Finance Committee

**Senate Health Education Labor & Pensions
Committee**

Senate Veterans Affairs Committee

SUBJECT: The Opportunity to Provide Meaningful Change for Health Sector Cybersecurity

Dear Mr. Kennedy, Senators and Representatives:

I am writing to you on behalf of HITRUST, the leading provider of cybersecurity and information security assurances, regarding proposed modifications to the HIPAA Security Rule under consideration by the Department of Health and Human Services (“HHS”, “Department”) and other bills under consideration in Congress seeking to implement new cyber security standards or requirements. As a longstanding leader in information security and cybersecurity risk management with 17 years of practical experience alongside measurable, and demonstrable results for the health industry, we have significant concerns that regulatory efforts will continue recent trends introducing requirements or practices that are not based on sound information security or risk management principles and create inefficiency and confusion for the healthcare system with limited measurable benefits.

The State of Healthcare Cybersecurity Guidance

Since the publication of the HIPAA Security Rule¹ over 20 years ago in 2003², multiple voluntary guidance programs have been attempted, such as the healthcare and public health sector response

¹ See <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es>.

² See <https://www.hhs.gov/hipaa/for-professionals/security/index.html>.

to the Cybersecurity Information Sharing Act of 2015³ through the 405(d) Program⁴ resulting in the publication of the Health Industry Cybersecurity Practices (HICP)⁵ for the healthcare and public health sector in 2019 among other outcomes. Subsequent to HICP, in January 2021, Congress enacted an amendment to the HITECH Act⁶ followed by video-only guidance⁷ from HHS's Office of Civil Rights ("OCR") in October 2022 which both defined a narrow interpretation of Recognized Security Practices ("RSPs") and chose not to consider the ways that the private sector has developed objective and measurable cybersecurity standards and assurance mechanisms valuable to achieving cybersecurity outcomes even where those efforts are recognized by statutory authorities outside the Federal Government and, most importantly, are proven to be highly effective. And, finally and most recently, in March 2023, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency ("CISA") released cross-sector cybersecurity performance goals with HHS subsequently publishing voluntary HPH CPGs⁸ in January 2024.

Unfortunately, while these efforts are laudable and seek to improve cybersecurity for the nation's healthcare industry, they did not address the risks, nor do they have the needed attributes of relevance and reliability. As such the attacks against the healthcare industry continue and remain highly effective. As we all know, both direct and opportunistic targeting continues and the healthcare industry unfortunately experienced significant events this year including a catastrophic and wide-ranging event that impacted the capability of the industry to provide and pay for life-saving care.⁹ The overall risk to our nation, in aggregate, is well beyond even that significant event. The healthcare sector has been the most "commonly victimized industry" in our country.¹⁰ Vital patient care is being impacted. And, according to the FBI, in 2023 the healthcare sector endured

³ See https://www.nist.gov/system/files/documents/2018/10/18/hhs_fact_sheet_-_csa_405d_cleared.pdf.

⁴ See <https://405d.hhs.gov/>.

⁵ See <https://405d.hhs.gov/cornerstone/hicp>.

⁶ See <https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf>.

⁷ See <https://www.youtube.com/watch?v=e2wG7jUiRjE>

⁸ See <https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf>.

⁹ U.S. Department of Health and Human Services (2024, Mar 5). HHS Statement Regarding the Cyberattack on Change Healthcare. Available from <https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html>.

¹⁰ Cybersecurity and Infrastructure Security Agency (2024, Feb 27). #StopRansomware: ALPHV Blackcat. Available from https://www.cisa.gov/sites/default/files/2024-02/aa23-353a-stopransomware-alphv-blackcat-update_1.pdf.

more ransomware attacks than any other critical infrastructure sector.¹¹ Since December 2023, healthcare companies have been the most victimized companies with hospitals named as a target by a major criminal actor.¹² The outcome of these events is a growing lack of trust in the cybersecurity posture of the healthcare industry with an impact to both patient engagement and provider effectiveness.¹³ The profound scope and reach of attacks and industry impacts requires a new approach.

The Opportunity to Leave Immature and Incomplete Approaches Behind

We believe in and align with a shared objective of the Department and the Congress that healthcare organizations must manage information risk effectively and that there need to be guidance or baselines established based on organization's risk and overall risk profile. Ultimately, we all must be confident that organizations and the industry as a whole are able to demonstrate that their compliance with effective risk management and cybersecurity requirements.

The requirements necessary to protect the health system and achieve cybersecurity requirements must be practical, understandable and stay relevant with changes in the (cyber) threat landscape and must also be measurable and reliable so that the company, industry peers and regulators who all rely upon the results have confidence in the level of assurance provided. The results must be trusted without regard to who performed the review.

In the current system, without regard to existing cybersecurity guidance as standards, published rules, practices, or goals, and whether the requirements are mandatory or voluntary, the outcomes we see prove that the approaches being used remain immature and incomplete. We find this disappointing as there are demonstrable and practical models that can be leveraged to improve both the cybersecurity risk and resilience of the healthcare industry.

¹¹ Federal Bureau of Investigation (2023, Mar 6). Internet Crime Report. Available from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

¹² Cybersecurity and Infrastructure Security Agency (2024, Feb 27).

¹³ Cyberattacks are undermining patient care and their trust (2024, Oct 11). Health Data Management. Available from <https://www.healthdatamanagement.com/articles/cyberattacks-are-undermining-patient-care-and-their-trust?id=135267>.

We respectfully suggest Congress and Department both specify methods that achieve the required outcomes, that are objectively measurable, maintain relevance and reliability while also being fully aligned with regulatory guidance and oversight objectives. This is fully achievable.

The goal of HIPAA and the Security Rule is to manage the risk to electronic protected health information and that goal has **never been achieved** because of a major design flaw. The HIPAA Security Rule and all of the subsequent efforts by the Government cannot reduce risk because they do not address the relevance of controls and assurance in any meaningful way. As a result, requirements are either 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.

Furthermore, our experience shows us that changes to current mandatory standards and regulatory requirements, such as the HIPAA Security Rule, must include several outcomes: (1) the opportunity to ensure that the changes are relevant to the threat landscape, (2) that the Rule is sufficiently prescriptive to achieve required outcomes while also preserving needed industry flexibility; (3) a system to provide objective measurement of security maturity and operational outcomes; (4) an approach that is capable of remaining aligned with a rapidly changing threat landscape on an ongoing basis which includes the rationale of changes as regular updates to the industry; and (5) an approach that leverages the scale of leading service providers such as cloud service providers and health industry software specialists to provide support for the entire healthcare system including underserved and underfunded elements.

More specifically:

1. Regulatory guidance must keep pace with the evolving cyber threat landscape and provide a mechanism where controls are constantly evaluated and enhanced to meet current and emerging cyber threats. Regulatory standards are unfortunately updated infrequently, and the process is insufficient to maintain pace with cyber threats. Using approaches that adapt actively is essential with changes to prescriptive requirements specified as threats evolve.

2. Assurance programs, which are absent today, should be expected and leveraged to validate that controls are not only in place, but are also effective and operationally mature. In addition, reciprocity with assurance systems from the private sector is required. This will provide needed scale and the ability to evolve with changing threats but must only be supported for programs that are transparent, scalable, consistent, accurate, and efficient—all essential for trust and integrity.
3. The models and approach used should meet the needs of all industry participants and not just presently regulated entities. The approach must begin with a specific set of good security hygiene and/or best/leading practices applicable to all organizations. Tailoring¹⁴ of additional control selections on top of those practices allows support for additional requirements and outcomes based on inherent risk and the approach needed to provide cyber security and resiliency for different size and classes of organizations. This model works because the eventual set of requirements are all backed and validated by the same transparent, consistent, accurate and efficient assurance system. This is especially important to the resilience of the healthcare system and other critical infrastructure industries where a subset of companies is the largest and most critical to the mission of the industry. This approach permits regulatory consistency without the ‘one size fits all’ approach that is inherently suboptimal due to differences in organizational complexity and maturity.

¹⁴ NIST defines tailoring as a process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. See NIST Online Glossary: Tailoring. Available from <https://csrc.nist.gov/glossary/term/tailoring>.

Objective Measurement and Outcomes

We have spent 17 years iterating this model to ensure relevance and reliability with many critical characteristics and we offer this a subset of our proven characteristics for consideration by the Department and Congress along with the risks they manage and implementation examples:

Characteristic		Risk Managed	Trust Report Reference
Cyber Threat Adaptive	<ul style="list-style-type: none"> • Mapping of threat intelligence data to threats through the MITRE ATT&CK framework • Use threat intelligence to identify the relevant controls needed to mitigate the threat and maintain security posture • Update control requirements actively and regularly 	<ul style="list-style-type: none"> • Risk of new threats emerging without relevant safeguards • Risk that compliance requirements no longer mitigate the active threat environment 	<i>Page 14 Relevant Control Framework</i>
Quantifiable Assurance	<ul style="list-style-type: none"> • Measure control maturity using a PRISMA-based control maturity and scoring model • Provide quantification of maturity characteristics against directly specified requirements 	<ul style="list-style-type: none"> • Risk that security requirements are not objectively evaluated • Risk that sustaining elements such as policies and procedures are not properly implemented 	<i>Page 18 Control Maturity Model</i>
Qualified and Objective External Assessors	<ul style="list-style-type: none"> • Provide training, qualification requirements, and testing for assessors • Separate qualification expectations for independent quality assurance personnel and the quality inspection requirements 	<ul style="list-style-type: none"> • Risk that assessors use proprietary and non-transparent testing protocols • Risk of inconsistent testing results and outcomes across different external assessors and assessment firms • Loss of independence and objectivity with testing and quality assurance performed by the same individuals 	<i>Page 16 Formal Assessor Program</i>
Centralized and Independent Quality Oversight	<ul style="list-style-type: none"> • Require independent quality testing and report issuance 	<ul style="list-style-type: none"> • Risk that results performed by different analysts and firms yield different outcomes based upon proprietary testing and validation protocols • Risk that the controls tested for the system are inconsistent with the business and technical outcomes delivered by the certified system • Risk that the outcomes measured do not align with regulatory and customer expectations 	<i>Page 17 Centralized Quality Assurance</i>

Characteristic	Risk Managed	Trust Report Reference	
Correction of Observed Issues and Identified Corrective Actions	<ul style="list-style-type: none"> • Register, document and track regular progress and mitigation of identified gaps and corrective action plans • Validate work completion as a component of maintaining certification 	<ul style="list-style-type: none"> • Risk that identified issues are not mitigated • Risk that changes in management of assessed entities lose sight of open and identified issues 	Page 27 <i>Annual Progress on Corrective Action Plans</i>

We know this works because we collect data to assess relevance and reliability and to continually improve our assurance system. Those metrics are available in our *2024 Trust Report*¹⁵ that publicly offers details and efficacy data for the HITRUST framework, assurance methodology, and related systems. Specifically, only 0.64% of HITRUST-certified environments at the Risk-Based, or r2, level reported breaches in 2022 and 2023. This metric is important as the ultimate outcome we seek is to mitigate information risk to an appropriate and acceptable level. That outcome is achieved because of controls that are relevant and specific enough to address identified threats and provide reliable assurance reports that test and that the controls are implemented and are made available to stakeholders, regulators and other relying parties seeking an understanding of the system including regulators.

Rigorous testing and risk reduction is an expectation of companies that seek a HITRUST certification and those that rely on our certifications. 72% of certified companies identify at least one corrective action which requires mitigation through their HITRUST assessment. And 92% of those issues are remediated within one year of their HITRUST assessment with assessed entities reporting their progress on their commitments. This demonstrates that these companies are committed to true accountability.

The efforts of industry participants that align with the system we offer are never done as security threats are continuously evolving. Our commitment to maintaining trust through relevance and reliability continues to guide our work and we offer our experiences as a model for the industry to follow. And healthcare companies large and small are responding. From 2022 to 2023, HITRUST has seen a 187% increase in our Leading Practices, or i1, validated assessment submissions and half of our new customers begin their security journey with the HITRUST Essentials, or e1,

¹⁵ See <https://hitrustalliance.net/trust-report>.

assessment. The leadership and commitment of these companies to cyber security is a good thing and is continually raising the bar through use of reasonable and appropriate security measures designed to address their most relevant threats.

Cyber Insurance Industry Engagement

Another important tool in responding to cyber threats is cyber insurance which helps companies respond when they are victims of attack. However, the ability to gain cyber insurance is both challenging and expensive after industry-wide events such as what the health industry is presently experiencing. HITRUST has been recognized by a syndicate of underwriters affiliated with Lloyds of London that will offer cyber insurance policies to companies that have demonstrated their commitment to cyber resilience through a HITRUST certification. This is very helpful to companies that regularly test their security programs and demonstrate their security maturity through our certifications beginning with our Risk-Based, or r2, certification.

Support for Rural Providers with Limited Technology and Cybersecurity Expertise

A challenge in health care is the diversity of access to leading technologies and limited security leadership across the breadth of the healthcare industry, both of which impede security adoption. For example, many health systems serve small or under-represented communities and may not have ready access to the expertise needed to keep up with security threats. As small and large organizations now heavily rely on cloud service providers for technology and cybersecurity needs, the use of such systems can accelerate cybersecurity capability adoption—today, 85% of the requirements for a HITRUST assessment may be inherited by health industry companies from a HITRUST certified cloud service provider¹⁶, such as Amazon AWS, Microsoft Azure, or Google Cloud. Making robust cybersecurity capabilities available to all healthcare industry organizations increases efficiency and reduces cost while streamlining security outcomes.

¹⁶ See <https://hitrustalliance.net/shared-responsibility-matrices>.

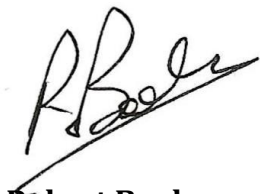
Closing

In closing, the health industry is not lacking in cybersecurity and information security standards, rules, practices and goals but is lacking in mechanisms that ensure (1) standards remain relevant to current and emerging cyber threats and (2) there are appropriate and reliable mechanisms to define, measure, and report on their implementation and effectiveness.

Ultimately, relevant controls must be implemented without regard to how they are specified and must also be tested to ensure they are implemented and operating properly to effectively mitigate risk. Relevant standards **with** reliable assurances provide trust and confidence through transparency that the appropriate controls are implemented and operating effectively.

We look forward to the Department's draft and fully intend to bring our expertise and 17 years of data certifying thousands of health systems to our comments and feedback. We are also committed to providing input to future legislative efforts including recent Bills being advanced to address cybersecurity needs for the health industry. For both the Department and Congress, our goal remains participation as an active party in supporting the best security outcomes for healthcare across our Nation.

Sincerely,

A handwritten signature in black ink, appearing to read 'R. Booker', written over a horizontal line.

Robert Booker
Chief Strategy Officer
HITRUST

Attachment: *2024 HITRUST Trust Report*
Also available at <https://hitrustalliance.net/trust-report>.