March 22, 2016

Healthcare Organizations Can Implement the NIST Cybersecurity Framework with HITRUST

CYBERSECURITY, DUE DILIGENCE , SOC
BY TIMOTHY WOLFGANG

Healthcare organizations face growing challenges in regards to protecting their patient information. Recent studies found that the healthcare sector had the highest cost per compromised record resulting from data breaches, while the cybercriminals can sell healthcare records for more than credit card and social security numbers, making them an increasingly attractive target. A robust cybersecurity program is a must for organizations that handle Personal Health Information (PHI), but how can you assess the adequacy of your current program or begin to implement one if it doesn't exist? The National Institute of Standards & Technology's (NIST) Cybersecurity Framework (CsF), a collection of cybersecurity standards, practices and guidelines, is a great tool. Healthcare organizations can find multiple benefits from its use, such as:

• Determining the activities that need to be completed to ensure that critical operations and service delivery are protected against cybersecurity risks.

• Prioritizing weaknesses, so the impact of cybersecurity investments can be measured and maximized.

• Allowing an organization to communicate it's cybersecurity posture to customers and interested parties.

• Compliance with HIPAA requirements by demonstrating commitments to due care and due diligence for the protection of PHI.

• Potential limitations in cybersecurity insurance premiums and breach liability.

One of the strengths of the NIST CsF is its adaptability to different industry sectors or organizations. However, organizations must invest resources in adapting it to their specific risks, situations and needs. For the healthcare sector, the Health Information Trust Alliance (HITRUST) has taken the lead and provided guidance on how healthcare organizations can implement a NIST CsF compliant cybersecurity program tailored to their needs through implementation of HITRUST's Risk Management Framework (RMF). HITRUST defines the following steps to implement the HITRUST RMF, a NIST CsF compliant program:

HITRUST'S RISK MANAGEMENT FRAMEWORK (RMF)

1. **Prioritize and scope** – Determine where your organization's sensitive assets (PHI)

reside and the risks to that information. Build an inventory of assets and classify them by sensitivity. Sources for identifying risks are regulatory guidance, industry publications and real-life breaches faced by similar companies.

2. **Orient** – Determine what cybersecurity and risk management practices are in place currently, what practices should be implemented, if not currently, and identify the critical systems where resources should be focused.

3. **Create a target profile** – Select a HITRUST control overlay and Target Tier for the organization. Target Implementation Tiers identify the specific controls and maturity of those controls needed to achieve the desired level.

4. **Conduct a cybersecurity risk assessment** – This is an evaluation of the organization's current controls and evaluation of the cybersecurity risks that are outside of desired tolerances based on the target profile. Some organizations may already have similar assessments in place through regular business processes such as Internal Audit Risk Analysis.

5. **Create a current profile** – This is a comparison of the Risk Assessment performed in Step 4 against the target profile performed in Step 3. The HITRUST framework can provide your organization's current profile in scorecard format, to identify the status and maturity of currently implemented controls.

6. **Conduct Gap Analysis** – A gap exists when the current control profile falls short of the control profile in the target profile. HITRUST provides several methods to prioritize the controls gaps an organization may have so resources can be allocated to areas with the strongest impact. In the first method, Risk, Likelihood and Impact ratings are calculated for each gap to give numeric values of the gap's overall risk level. In the second method, priority codes are given to controls, signifying which control gaps should be closed first to allow other controls to build upon them.

7. **Implement an Action Plan** - Execute a plan to track all projects related to closing identified gaps and monitor their status against the desired target profile. Repeat the steps.

Organizations wishing to reap the benefits of the HITRUST (RMF) can complete these steps themselves (self-assessment) or engage a HITRUST Assessor to provide experienced guidance and assurance. Only HITRUST Assessors can provide an organization with a HITRUST validated certification. In addition to providing certification, HITRUST Assessors can provide a HITRUST standard report or SOC2 Plus report with HITRUST that can be provided to customers and interested parties who inquire about an organization's security and privacy practices.

If your organization already has the HITRUST RMF implemented and is interested in the NIST Csf, HITRUST has published control mappings that can be used to demonstrate compliance based on activities already in place. Alternatively, the mappings can be used by organizations with the NIST CsF in place to gain HITRUST certification. The HITRUST guide to implementing the NIST CsF and the control mappings can be found here.

Schneider Downs can assist healthcare organizations and business associates wishing

to incorporate HITRUST and the NIST CsF into their business activities and report on those activities via SOC2 Plus with HITRUST, please contact us for more information.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.