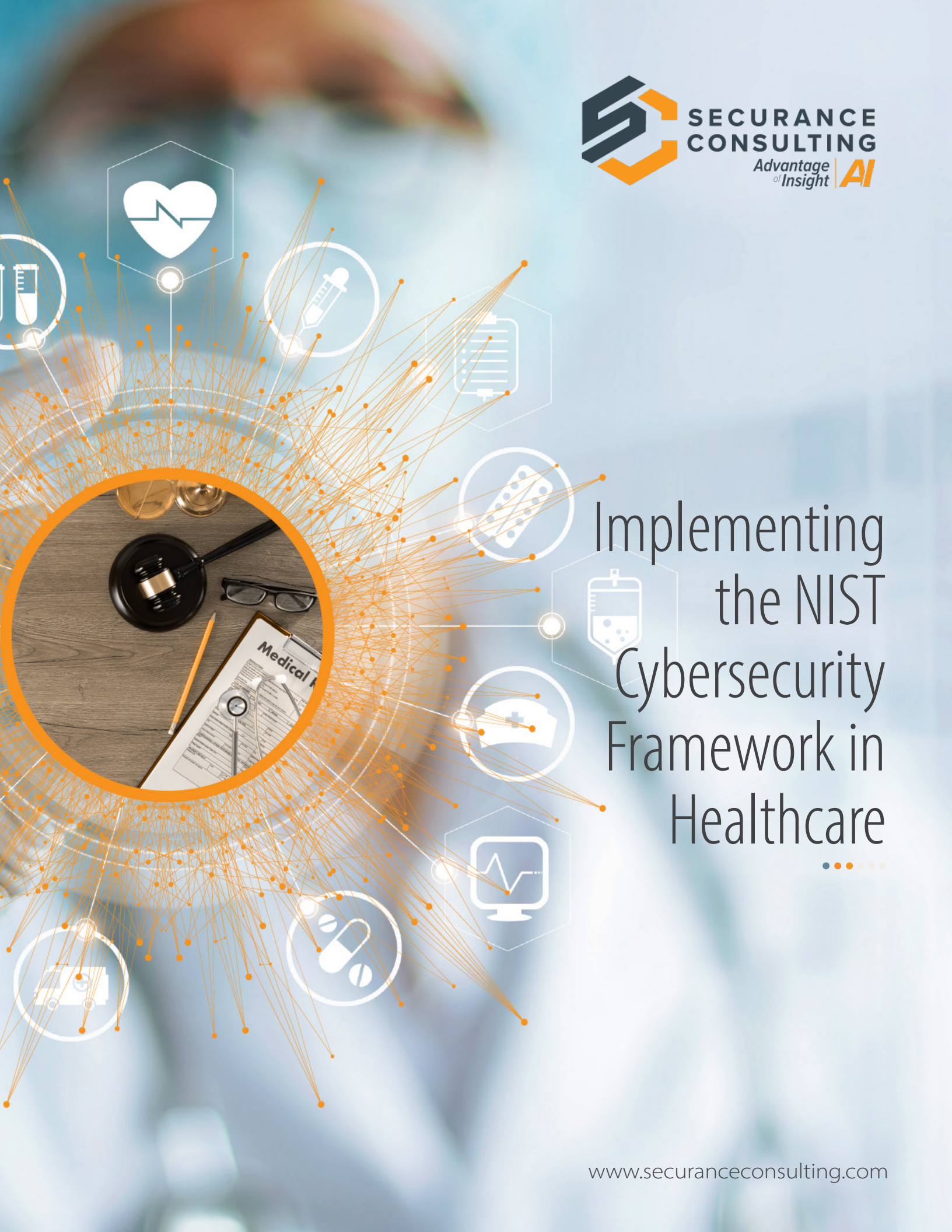
SECURANCE CONSULTING
Advantage of Insight AI



Implementing the NIST Cybersecurity Framework in Healthcare

www.securanceconsulting.com

THE CHALLENGE AND ITS SOLUTION

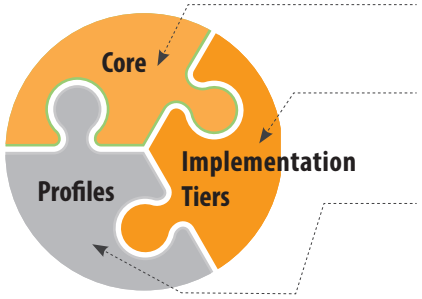
Healthcare is a heavily regulated industry, with state, local, and federal mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH), setting specific standards to protect the privacy and security of physical and electronic protected health information (PHI).

The problem with HIPAA is that, while it tells healthcare providers *what* they should comply with, it doesn't tell them *how*.

To adequately protect data, organizations must instate effective information security measures, a process made easier by following a trusted security framework like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This set of standards provides a cohesive framework and starting point for organizations to implement information security controls covering user access, infrastructure, and physical security— making compliance initiatives much easier to understand and prioritize.

Functions of a Cybersecurity Framework

Components of the NIST CSF



Enables communication of cybersecurity risks across an organization

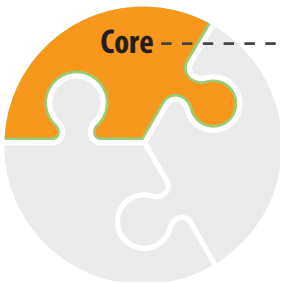
Determine the desired level of thoroughness for a security program

Align industry standards and best practices, and support prioritization and measurement

WHAT IS THE NIST CSF?

The NIST CSF was originally developed under an executive order to improve the security of critical infrastructure, defined as any "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" by the Patriot Act of 2001. The definition intentionally does not refer to specific industries, in order to express the varied nature of those systems and assets that might be critical to national security. Due to the framework's wide applicability, its use has expanded to many other industries outside of critical infrastructure. Today, organizations of all sizes and purposes leverage the NIST CSF to understand and manage cybersecurity risks.

There are five Functions that comprise the framework's Core:



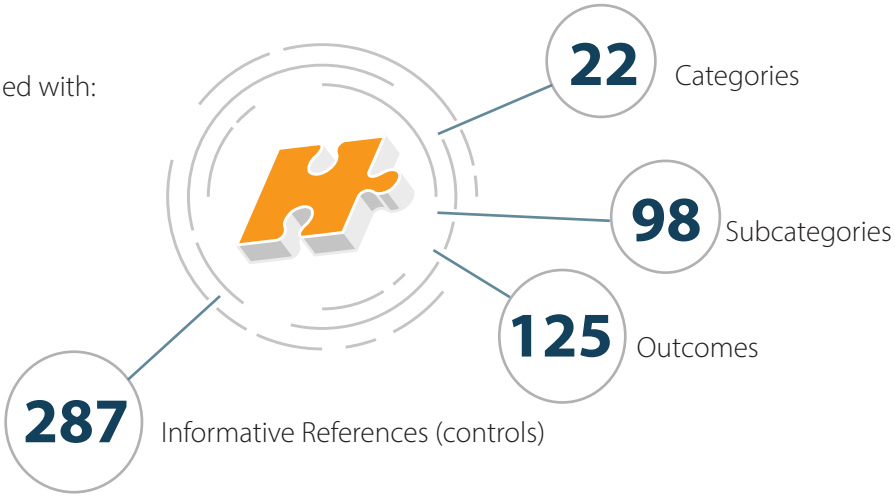
Identify: Understand how to discover and manage cybersecurity risks
Protect: Support the ability to limit or contain the impact of cybersecurity events
Detect: Identify cybersecurity events
Respond: Take action after detecting a cybersecurity event
Recover: Repair and restore services affected by cybersecurity events

While the NIST CSF was not specifically created for the healthcare sector, it provides guidance for establishing relevant programs and policies, as well as overcoming security challenges.

Organizations hoping to use the NIST CSF as a simple checklist, however, will be disappointed. The framework provides not a list of security controls to implement, but rather, high-level best practices and recommendations to improve security maturity and increase visibility into systems, networks, and data.

The NIST CSF is not a maturity model. Even so, many organizations use it as such, because its four Tiers provide context around how entities view cybersecurity risk and the processes in place to manage that risk. The Tiers are: Partial, Risk-Informed, Repeatable, and Adaptive.[2]

The Core's Functions are aligned with:



BENEFITS OF IMPLEMENTING THE NIST CSF

As previously mentioned, the NIST CSF can help healthcare providers align with HIPAA and other compliance regulations by offering an organized framework that defines cybersecurity maturity and heightens awareness of important components of the security program. These benefits alone are a boon to organizations strapped for time and resources, but they aren't the only advantages to implementing the NIST CSF. Other benefits include:

1. Protection of electronic medical records from common cybersecurity risks, such as malware, ransomware, and malicious insider attacks
2. Identification of healthcare technologies to implement to improve overall security
3. Identification of cybersecurity training opportunities for staff
4. Alignment of IT and healthcare goals and policies
5. Prioritization of cybersecurity tasks and resource allocation
6. Helps develop a long-term plan to address cybersecurity risks
7. Encourages a proactive, rather than reactive, approach to security
8. Discourages a "check the box" approach to HIPAA compliance and cybersecurity
9. Enables organizations to easily integrate new regulations
10. Facilitates stakeholder understanding of cybersecurity and how to manage risks
11. Provides visibility into business requirements, financial capabilities, and risk tolerance
12. Helps providers identify, detect, and recover from security threats

> The NIST CSF is not a standalone framework. It is designed to be paired with other frameworks, such as ISO/IEC 27000, COBIT 5, ANSI/ISA 62443, and NIST SP 800-53.

Guidance released in 2015 and updated in 2016 by the Health Information Trust Alliance (HITRUST) summarizes the benefits of implementing the NIST CSF as follows: "Based on a collection of cybersecurity standards and industry best practices, the NIST CSF broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes, the Framework can facilitate improvements in cybersecurity and the resilience of critical infrastructure."

Specifically, the NIST CSF:

- Provides guidance on risk management principles and best practices
- Provides a common language to address and manage cybersecurity risk
- Outlines a structure for organizations to understand and apply cybersecurity risk management principles
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs."[4]

HITRUST also notes other potential benefits of leveraging the NIST CSF:

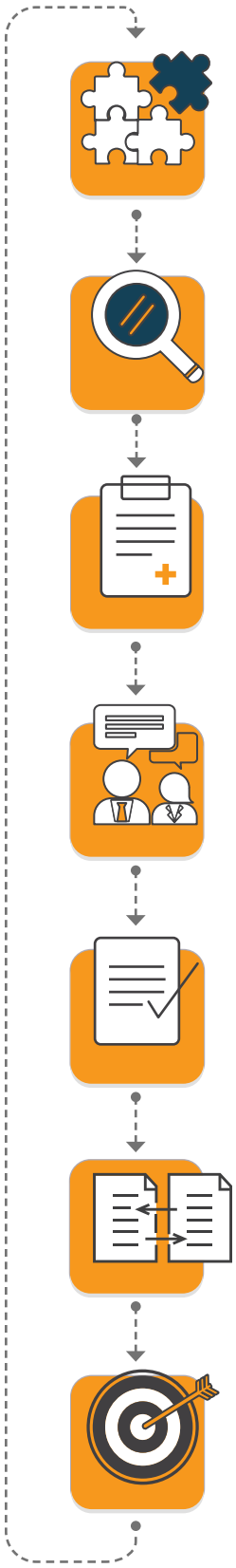
- Formal recognition by the federal government
- Limitations in breach liability
- Reductions in cybersecurity insurance premiums
- Increased likelihood of receiving grants through federal programs
- Prioritized federal government technical assistance

How to implement the NIST CSF

A helpful resource for those about to implement the NIST CSF is the HITRUST Healthcare Sector Cybersecurity Implementation Guide that was developed to help healthcare organizations (more specifically, their leadership) to:

» Understand NIST CSF terminology, concepts, and benefits
» Assess their current and targeted cybersecurity postures
» Identify gaps in their current programs and workforce
» Identify current practices that meet or exceed NIST CSF requirements

> Only **44%** of healthcare providers, including hospital and health systems, conformed to protocols outlined by the NIST CSF."[3]



The framework provides a cyclical seven-step implementation process:

Step 1 – Prioritize and scope: Identify business objectives and high-level organizational priorities in order to strategically prioritize cybersecurity initiatives and determine the scope of systems and assets that support core business processes.

Step 2 – Orient: Identify systems and assets, regulatory requirements, and the overall risk approach, then find threats and vulnerabilities related to those systems and assets.

Step 3 – Create a current profile: Indicate which Category and Subcategory outcomes from the CSF Core are currently being achieved.

Step 4 – Conduct a risk assessment: Evaluate the operational environment to determine the likelihood and impact of experiencing a cybersecurity event, including emerging risks and threat and vulnerability data.

Step 5 – Create a target profile: Indicate which Category and Subcategory outcomes from the CSF Core the organization would like to achieve.

Step 6 – Determine, analyze, and prioritize gaps: Compare the current and target profiles to identify gaps, create an action plan, and define the resources required to address gaps.

Step 7 – Implement action plan: Decide which actions to take, and which standards, guidelines, and practices to implement, to close gaps between the current and target profiles.[5]

This process is repeatable, so providers can continually assess their cybersecurity measures and update their cybersecurity programs to meet current needs.

CONCLUSION

More often than not, when we talk about healthcare, we talk about HIPAA— but that isn't all there is to healthcare cybersecurity. Because no two healthcare organizations are the same or have an identical set of needs, HIPAA guidelines are intentionally vague, requiring organizations to seek help when implementing "reasonable and appropriate" safeguards for PHI.

The NIST CSF, while intentionally vague in its own right, provides a sturdy foundation for healthcare providers to implement the standards necessary to achieve HIPAA compliance. It uses risk management processes to enable organizations to prioritize decision-making and inform process implementations. Its encouragement of continuous assessment also helps organizations keep risk management at the forefront, which ensures protection of PHI over the long term.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://securityboulevard.com/2020/02/cybersecurity-frameworks-in-healthcare-and-how-to-adopt-them/
2. https://www.securitymagazine.com/blogs/14-security-blog/post/88890-how-to-use-the-nist-cybersecurity-framework
3. https://www.helpnetsecurity.com/2020/09/22/healthcare-providers-nist-csf-protocol/
4. https://hitrustalliance.org/documents/cybersecurity/HPHCyberImplementationGuide.pdf
5. https://us-cert.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

Implementing the NIST Cybersecurity Framework in Healthcare

SECURANCE CONSULTING
Advantage of Insight AI

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com