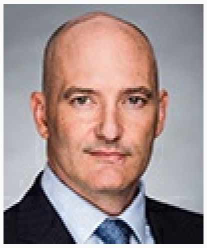
# Compliance Today - May 2022
# A proactive approach to cybersecurity: Adopting best practices is critical

By Jon Moore, MS, JD, HCISPP

**Jon Moore** (jon.moore@clearwatercompliance.com) is Senior Vice President and Chief Risk Officer, Clearwater, Nashville, TN.


Jon Moore

For far too long, many healthcare organizations viewed cybersecurity as a problem exclusively for their IT departments. Leaders at these organizations failed to appreciate how a single cyber incident could have lasting—and potentially devastating—consequences for the organization as a whole, its patients, and partners.

Unfortunately, many healthcare executives and their boards are now learning the hard way that data privacy and security are no longer just technical issues for the IT team that are hidden behind complicated jargon.

In 2021, the Office for Civil Rights (OCR) investigated a record number of breaches. Its breach portal shows 714 reported breaches of protected health information affecting records of 500 or more individuals for that year.[1] This represents a 7.7% increase over the previous year. Ten of those incidents exposed a million or more records each. As of March 10, there have been an additional 102 reported breaches of 500 or more records and another million-plus record breach.

These breaches are costing healthcare a record-breaking amount of money. IBM's*Cost of a Breach Report 2021*[2] cites healthcare again at the top of the list—for 11th consecutive year—as the industry with the highest average cost of a breach. In 2021 that average cost reached $9.23 million, compared to $7.13 million in 2020. With the number of successful breaches last year—reflective of what we've seen since the onset of the pandemic—it wouldn't be surprising, when the numbers are tallied for the 2022 report, to see it continuing to rise.

That's why it's becoming ever more apparent that healthcare organizations can no longer approach cybersecurity reactively and as simply an IT problem.

Today, the most successful healthcare organizations take a more proactive and holistic approach to their cybersecurity and risk management programs. They understand that now is the time to adopt best practices and better prepare themselves for the increasing likelihood of attacks and incidents.

The good news is that there are now many incentives to take action, and with proper guidance and support, your organization can be well on its way to reducing your cyber risks today and in the future.

## New incentives, new motivations

While there are many practical reasons to invest time and resources to implement more robust cybersecurity practices, some healthcare organizations might not be aware of a new law that provides even more incentive to do so—HR 7898.[3]

HR 7898 became law last year. It's an amendment to the Health Information Technology for Economic and

Clinical Health (HITECH) Act that encourages healthcare-covered entities and their business associates to adopt recognized cybersecurity practices. How? Because if you experience a breach or other security incident and get on the U.S. Department of Health & Human Services' radar, demonstrating your healthcare organization has recognized cybersecurity practices in place must be taken into consideration when the agency reviews your case.

While it's not a safe harbor and won't protect you from fines, penalties, or other measures, it may affect how long an audit lasts, what its outcome might be, and could potentially influence the amount of fines and other penalties you face.

**The law specifies:** "*Nothing in this section shall be construed to limit the Secretary's authority to enforce the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title), or to supersede or conflict with an entity or business associate's obligations under the HIPAA Security Rule.*"[4]

But the law does instruct OCR to consider whether, if the healthcare organization has demonstrated that for the preceding 12 months, it has recognized cybersecurity practices in place.[5]

In simplest terms, OCR may still impose fines and penalties. Still, healthcare organizations that have adopted recognized practices may experience far less scrutiny and reduced monetary penalties. As a healthcare covered entity or business associate, the incentive here is if you do face an audit or have a security incident that prompts an investigation, you may experience a range of advantages you'd otherwise miss out on.

## Setting best-practice expectations

So, how does HR 7898 define "recognized security practices," and what does that mean for your organization?

As defined by statute, HR 7898 defines recognized security practices as:

> Standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

While the statute is a bit vague, currently there are two practices typically cited as meeting the requirement of recognized security practices under HR 7898:

1. National Institute of Standards and Technology (NIST) Cybersecurity Framework,[6] developed under the statutory authority of Section 2(c)(15) of the NIST Act, and

2. Health Industry Cybersecurity Practices (HICP),[7] published as voluntary guidance by the 405(d) Program and Task Group—a collaborative effort between industry and government under the Healthcare and Public Health Sector Coordinating Council Joint Cybersecurity Working Group.

The NIST Cybersecurity Framework is a set of security activities and informative references that help organizations of all sizes and industries better analyze, address, and manage risks across their enterprise. It assists organizations in identifying a target cybersecurity profile that describes a cybersecurity program that is reasonable and appropriate for the organization, measuring where the organization is currently relative to that target profile, and plotting a course to achieve the target.

Cybersecurity Act of 2015, Section 405(d), "Aligning Health Care Industry Security Approaches," was designed to create "voluntary, consensus-based, and industry-led guidelines, practices, methodologies, procedures, and processes" that:

- Help healthcare organizations cost-effectively reduce cyber risks;
- Encourage adoption and implementation of measures to address cyber risk; and
- Remain consistent with NIST, HIPAA, and HITECH.

The 405(d) Program and Task Group met this obligation with the development, publication, and promotion of HICP. The HICP documents:[8]

1. Examine current cybersecurity threats affecting the health and public health sector,
2. Identify specific weaknesses that make organizations more vulnerable to the threats, and
3. Provide selected practices across 10 areas that cybersecurity experts rank as the most effective to mitigate the threats.

Some commentators have suggested that other industry frameworks also meet HR 7898 requirements. The idea behind this belief is that these other frameworks are mappable to the NIST Cybersecurity Framework, and NIST publishes them as informative references.

However, it's not clear whether just because NIST accepts a framework as an informative reference, U.S. Department of Health & Human Services should view it as a recognized security practice under HR 7898. In fact, NIST states explicitly: "Disclaimer: Informative References are linked to by NIST for informational purposes only and do not constitute an endorsement by NIST of the submitted content."[9]

Since there is some ambiguity here, if your organization hopes to reap the benefits that may be afforded to you through HR 7898, stick with the NIST Cybersecurity Framework or Section 405(d) HICP.

## Putting the NIST Cybersecurity Framework to work for you

What might adoption of the NIST Cybersecurity Framework look like for your organization? One of the many benefits of this framework is its flexibility. NIST provides a common organizational structure for various approaches to cybersecurity. It is also mapped to a range of international standards. Your organization can pick and choose which standards to adopt based on your needs and goals. And, because there is no hierarchy of controls, you can apply standards that meet your needs today and then layer in additional ones as your organization evolves.

Let's take a quick look at the NIST Cybersecurity Framework Core. First, there are five functions aligned to the cybersecurity life cycle:[10]

1. **Identify**: "Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."
2. **Protect**: "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."
3. **Detect**: "Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

4. **Respond**: "Develop and implement the appropriate activities" when a cyber event is detected.
5. **Recover**: "Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

Within each of the five core functions, there are additional categories. These are groups of cybersecurity outcomes connected to specific program needs and activities. There are 22 total categories across the five functions. Here's what they look like:[11]

1. **Identify**
    1. Asset management
    2. Business environment
    3. Governance
    4. Risk assessment
    5. Risk management strategy
2. **Protect**
    6. Identity management and access control
    7. Awareness and training
    8. Data security
    9. Information protection processes and procedures
    10. Maintenance
    11. Protective technology
3. **Detect**
    12. Anomalies and events
    13. Security continuous monitoring
    14. Detection processes
4. **Respond**
    15. Response planning
    16. Communications
    17. Analysis
    18. Mitigation
    19. Improvements

5. **Recover**
    20. Recovery planning
    21. Improvements
    22. Communications

The NIST Cybersecurity Framework goes even deeper in helping guide organizations by further dividing each of the 22 categories into specific subcategories that define particular outcomes or technical and management activities.

Here's a quick perspective of how one of these functions, down through a category and subcategory, might look for your healthcare organization:

- Function: Identify
    - Category: Asset management
        - Subcategory: Catalog external information systems

Your organization's target profile will align functions, categories, and subcategories from the NIST Cybersecurity Framework with your specific organizational goals and objectives, such as your unique business requirements, risk tolerance levels, compliance requirements, and other needs and resources for your business. You can use this profile to build a road map for your cybersecurity program that will help lead you from your current posture to where you want to be over time.

## HIPAA mapping

In addition to maturing your cybersecurity practices by implementing a framework such as NIST's, you can also get better insight into your HIPAA Security Rule compliance. When developing your target profile, your organization can include HIPAA-required security practices into that profile. When comparing where you are relative to the profile, gaps in compliance may be found.

This type of mapping can help you understand all of your compliance requirements. It can help measure performance and identify security gaps before you experience a breach. It can also help identify noncompliance before a regulatory body cites you or a valued partner calls into question your meeting of contractual requirements. You can also use this approach to better understand, assess, and manage your organization's risks and risk profile.

## The NIST Cybersecurity Framework working together with Section 405(d)

One common complaint about the HIPAA Security Rule is that organizations are left to guess what reasonable and appropriate safeguards mean for their organization.

The HICP technical volumes produced under Section 405(d) perhaps provide some guidance on what is reasonable and appropriate not just generally but also by size and type of organization. They do this by defining small, medium, and large organizations and providing recommended security controls in 10 areas for each organization size.

In addition, these recommendations are mapped to the NIST Cybersecurity Framework. This facilitates including them into an organization's target profile, guiding the development of the target, and allowing an organization to adopt both the NIST Framework and Section 405(d) together.

## Takeaways

- Among the many benefits of implementing the NIST Cybersecurity Framework and drawing on recommendations from Section 405(d) of the Cybersecurity Act of 2015 Health Industry Cybersecurity Practices is how together these two important tools can help facilitate cyber-readiness conversations between your information security team and your executives and key stakeholders.
- These conversations are often overlooked, but they're increasingly crucial to help frame your cybersecurity program in a way that protects and secures your sensitive data and aligns it to your organization's overall goals and objectives. It can help facilitate these types of discussions at all levels of your organization.
- For example, you can use the five core functions of the NIST Cybersecurity Framework to give your board members and key stakeholders a high-level look at your cybersecurity program, your goals, and why it's a crucial component of managing the organization's overall enterprise risk posture.
- From there, you can go deeper with your executives. For example, you could break down those 22 related categories and what they mean for your organization (or what not having them could mean for your organization in terms of potential breach impact, fines, and penalties) with your executive leadership team.
- Then, continuing across the NIST Framework, you can draw on subcategories and individualized controls as a basis of conversation and goal-setting for the teams charged with managing and maintaining these activities on an ongoing basis.

[1] "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health & Human Services, accessed March 10, 2022, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[2] IBM, *Cost of a Data Breach Report 2021*, accessed March 10, 2022, https://www.ibm.com/security/data-breach.

[3] To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. L. No. 116-321, 134 Stat. 5072 (2021), https://www.congress.gov/bill/116th-congress/house-bill/7898.

[4] To amend the Health Information Technology for Economic and Clinical Health Act, 134 Stat. 5073.

[5] To amend the Health Information Technology for Economic and Clinical Health Act, 134 Stat. 5072.

[6] "Cybersecurity Framework," National Institute of Standards and Technology, accessed March 10, 2022, https://www.nist.gov/cyberframework.

[7] "HHS 405(d) Aligning Health Care Industry Security Approaches," U.S. Department of Health & Human Services, accessed March 10, 2022, https://405d.hhs.gov/public/navigation/resources.

[8] U.S. Department of Health & Human Services, Healthcare & Public Health Sector Coordinating Councils,*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, accessed March 10, 2022, https://405d.hhs.gov/Documents/HICP-Main-508.pdf.

[9] "Informative References," Cybersecurity Framework, National Institute of Standards and Technology, updated August 5, 2020, https://www.nist.gov/cyberframework/informative-references.

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018, 45–46, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[11] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 7–8.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login