Clearwater

Whitepaper

The Guide to 405(d) Health Industry Cybersecurity Practices

Table of Contents

Introduction 3

The role of the 405(d) task group 3

Why we need 405(d) HICP 5

Does PL 116-321 provide regulatory relief? 5

A closer look at 405(d) HICP 7

Practices and sub-practices 9

Two new recommendations in the 2023 HICP guide: 10

How to use 405(d) HICP 11

Reaping the benefits of 405(d) HICP 14

Introduction

In January 2021, HR 7898 became law as an amendment to the Health Information Technology for Economic and Clinical Health Act (HITECH Act). In simple terms, HR 7898 (now Public Law 116-321) requires the U.S. Department of Health and Human Services (HHS) to recognize the adoption of cybersecurity best practices.

From a HIPAA perspective, this new law isn't a safe harbor for healthcare organizations or their business associates (BA). If the Office for Civil Rights (OCR) finds your organization in violation of a HIPAA mandate, you'll still be subject to an audit or investigation, along with potential fines, penalties, and other possible punitive actions, including the potential for civil or criminal actions.

What PL 116-321 may do, however, is give your organization some grace when it comes to how long an OCR audit may last as well as its potential impact.

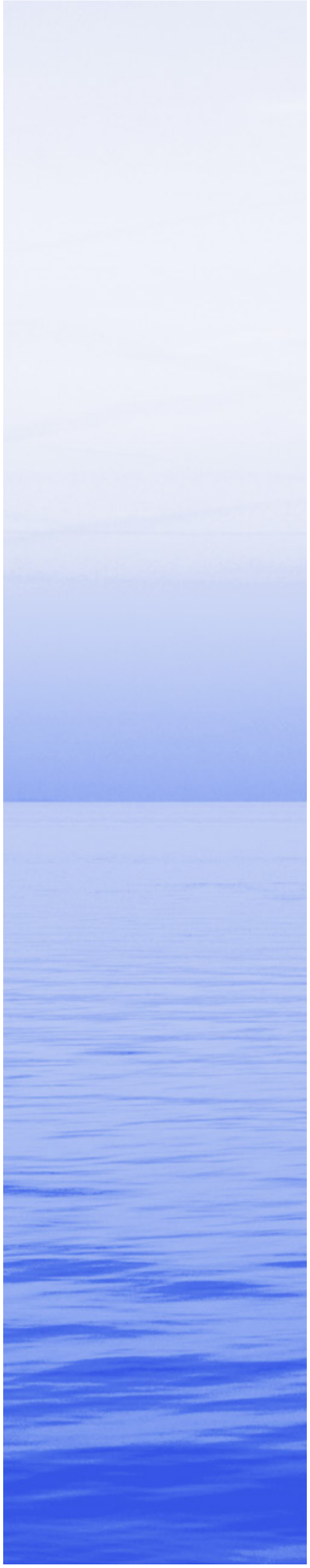
When it comes to PL 116-321, we're talking about specific cybersecurity practices. PL 116-321 identifies these security practices from "section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities."

These security practices include the NIST Cybersecurity Framework (NIST CSF) and what we're now commonly referring to as 405(d) Health Industry Cybersecurity Practices (HICP), which are mapped to NIST CSF.

The role of the 405(d) task group

Congress mandated the Cybersecurity Act of 2015. CSA includes Section 405(d): Aligning Health Care Industry Security Approaches. The CSA of 2015 established the creation of the Healthcare Industry Cybersecurity Task Group, which today can help with additional guidance and support for 405(d) expectations.

As a result, in 2017, HHS convened the 405(d) Task Group, leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. That task group comprised 200 information security officers, medical professionals, privacy experts, and industry leaders.



"Section 405(d) of the Cybersecurity Act of 2015 called for a more coordinated approach to cybersecurity in the healthcare industry. Supporting that mission, in 2018, HHS issued voluntary cybersecurity guidance for healthcare entities ("Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients") based on the recommendations of the 405(d) Task Group, an HHS and industry-led collaborative task group." Ref: Emily Poole, Alston & Byrd

Together, they had a goal to develop consensus-based guidelines, practices, and methodologies to strengthen healthcare against cyber threats, including:

- Cost-effectively reduce cybersecurity risks for a range of healthcare organizations
- Support voluntary adoption and implementation
- Ensure on an ongoing basis that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level.

What is the Cybersecurity Act of 2015 (CSA)?

The Cybersecurity Act of 2015 (CSA) (Public Law 114-113) establishes a trusted platform and a tighter partnership between the United States (U.S.) government and the private sector, recognizing that our critical infrastructure, economic solvency, and personal safety have become intertwined with our digital technologies.

Why we need 405(d) HICP

When HIPAA became law back in 1996, we didn't know a lot about cybersecurity as an industry. Processes and frameworks were still being developed, as they have been during the past 20-plus years.

As a result, those HIPAA guidelines didn't consider an organization's capabilities, resources, or threats. Today, 405(d) HICP helps clarify some of that ambiguity. Regarding cybersecurity best practices, 405(d) HICP looks at them through a lens that recognizes small, medium, and large organizations.

This is particularly critical in the changing face of healthcare due to the coronavirus pandemic, which has altered the way most healthcare organizations deliver health-related services. We're seeing a growing number of successful breaches resulting, in some instances, in the exposure of millions of records in a single breach. These attacks disrupt healthcare personnel's abilities to provide life-changing and life-saving capabilities.

Cybersecurity has been a big issue in healthcare for years, even before the pandemic. Still, now, with PL 116-321 and 405(d) HICP, we have some alignment between the government and the private sector in terms of best practices to protect this part of the critical infrastructure.

This aligns organizations of all sizes toward a common goal: to develop guidelines and practices that can best be used against the industry's current cybersecurity threats.

Most industry experts see 405(d) HICP as welcomed guidance and resources, eliminating some of the subjective direction that has long surrounded HIPAA compliance.

Does PL 116-321 provide regulatory relief?

PL 116-321 doesn't provide any regulatory relief regarding HIPAA compliance; however, it offers much-needed alignment and guidance between NIST CSF and 405(d) HICP.

As a healthcare provider or BA, you must still comply with HIPAA, so you must do a HIPAA risk analysis to adequately respond to your risks and address other security aspects of HIPAA. 405(d) HICP does provide some mitigating factors to HIPAA requirements.

What is 405(d)?

Section 405(d) of CSA calls for "Aligning Health Care Industry Security Approaches." It is with this imperative that industry and government came together under the auspices of the 405(d) Task Group, starting in May 2017. The Task Group focused on building a set of voluntary, consensus-based principles and practices to ensure cybersecurity in the Health Care and Public Health (HPH) sector. This document reflects the Task Group's current recommendations.

If you can demonstrate the adoption of federally recognized security practices for a period of at least 12 months prior to a violation, it could mitigate fines, assist in terminating an audit, or mitigate validation remedies. PL 116-321 through NIST CSF and 405(d) HICP provide very specific control guidance, stating: "The Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may mitigate fines under section 1176 of the Social Security Act (as amended by section 13410); result in the early, favorable termination of an audit under section 13411; and mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title) between the covered entity or business associate and the Department of Health and Human Services."

A closer look at 405(d) HICP

According to HHS, the top current threats for healthcare include:

- Email phishing attacks*
- Ransomware attacks
- Loss or theft of equipment or data
- Internal, accidental, or intentional data loss
- Attacks against connected medical devices that may affect patient safety

*2023 Update: Email phishing was updated to social engineering in the 405(d) HICP 2023 edition to encompass similar threats like smishing, whaling, business email compromise, and more. Social engineering refers to an attempt to trick someone into giving out personal information or infecting a device by clicking on a link that gives hackers access to various sources of data.

As such, 405(d) HICP provides guidance regarding vulnerabilities, impact, and safeguards against these and other threats. It's designed to help healthcare organizations design and implement effective cybersecurity objectives and outcomes.

405(d) HICP includes one main document and two technical volumes.

The main document explores the five top threats listed above and offers 10 best practices healthcare organizations can employ to mitigate those threats.

Technical Volume 1 takes those 10 practices and breaks them down in an applicable way for small healthcare organizations.

Technical Volume 2 explores 10 cybersecurity practices that fit medium and large healthcare organizations.

Those practices are:

1. Email protection systems
2. Endpoint protection systems
3. Access management
4. Data protection and loss prevention
5. Asset management

6. Network management
7. Vulnerability management**
8. Incident response
9. Medical device security
10. Cybersecurity policies**

**2023 updates to practices and sub-practices:

- Practice #9 has been fully updated with new sub-practices to account for the growing use of connected medical devices.
- Practice #10 has been updated to Cybersecurity Oversight and Governance to account for the oversight and governance structures that organizations should have as part of their cybersecurity programs.
- Cybersecurity Insurance is a new sub-practice under Practice #10. With the prevalence of cyberattacks on healthcare organizations, cybersecurity insurance has become an important component of your overall cyber risk management strategy. The HICP guidelines offer information on what your insurance policies should cover.
- Cybersecurity Risk Assessment and Management is a new sub-practice under Practice #10: The new HICP edition now includes guidance on how to perform risk assessments and offers free federal tools you can use to perform them on your own.
- Attack Simulation is a new sub-practice under Practice #7. The guidelines stress the importance of simulating attacks to test your controls and safeguards and outline what to include in your simulations.

Prioritization is a crucial part of practice guidance. Essentially, the 10 practices help healthcare organizations understand how to achieve outcomes identified in the NIST CSF, tailored to healthcare.

So, if you're a small healthcare organization, you can start with Volume 1; however, if you scale, then Volume 2 may help you mature your cybersecurity practices. Where you fit today may not be the same later if you grow.

In addition to your organization size, you may have a different maturity workflow across your enterprise. Some examples of that may be, for example, if you acquire another practice. First, you may fall under the practice guidelines of a small organization, but after the acquisition, you may need to advance to technical guide 2 for medium or large.

Just remember, as your healthcare organization grows through 405(d) HICP, it's likely you'll need a higher level of controls. So, when you look at your cybersecurity program, you'll need to consider using this as a foundation or alignment. Consider the maturity workflow because where you are now may be different as your organization grows or changes.

Regardless of organization size, you must still comply with HIPAA, but 405(d) HICP now provides additional and very detailed guidance on how to achieve that.

Practices and sub-practices

Section 405(d) includes practices and sub-practices healthcare organizations can apply based on organization size. When you look at those volumes that impact small, medium, and large organizations, you'll see those top threats outlined to various controls to mitigate the threats. The practices are at a higher level, while the sub-controls go into more detail. These practices and sub-practices can help guide your actions and investments into your healthcare cybersecurity program.

The practices are designed to help strengthen cybersecurity capabilities by:

- Enabling organizations to evaluate and benchmark cybersecurity capabilities effectively and reliably.
- Sharing knowledge, common practices, and appropriate references across organizations to improve cybersecurity competencies.
- Enabling organizations to prioritize actions and investments—knowing what to ask—to improve cybersecurity.

Each volume adds sub-practices based on organization size and builds off the previous area.

Let's look at the sub-practices by organization size for email protection systems. For small healthcare organizations, there are three related sub-practices: email system configuration, education, and phishing simulation. For email system configuration, a small healthcare organization should consider controls to enhance email security, such as avoiding free or "consumer" email systems and ensuring you have basic spam/antivirus installed, active, and automatically updated.

For a medium-sized healthcare organization, the sub-practices go into more detail, including basic email protection controls, multi-factor authentication for remote email, email encryption, and workforce education.

Large organizations can build on that further by developing email protection systems that use advanced and next-generation tooling, digital signatures, and analytics-driven education.

It's recommended that your organization use its risk analysis processes to help identify and prioritize the rollout of these controls.

One of the many benefits of 405(d) HICP is the higher level of specificity to help drive appropriate conversations, guide proper investments into your security model, and help provide clarity about how you should invest in your cybersecurity controls. And, you get the added benefit of having these controls already mapped to those relevant and common healthcare threats.

Two new recommendations in the 2023 HICP guide:

The 405(d) HICP 2023 edition also highlights two recommended practices every covered entity and business associate should consider as part of their overall cybersecurity strategy:

1. Zero Trust: Building a zero trust architecture encompassing multi-layer protections strengthens your security posture. This means validating all device and user identities, both internal and external, before granting access to network resources. You can use this approach to mitigate vulnerabilities that network trends create, including bring your own device (BYOD), cloud-based services, and remote workers. Your organization can enable a zero trust strategy at all network levels to ensure a strong security posture. Implementing an access and identity management solution and leveraging a least-privilege access process together are good starting points to a zero trust model.

2. Defense in depth: A holistic cybersecurity approach, such as defense-in-depth, can slow attacks and minimize damage. Defense-in-depth layers multiple security safeguards rather than relying on a single layer. If one layer is inadequate, another layer will hopefully prevent a full breach. This is a best practice strategy you can implement in different ways (for different

entity sizes) based on relevance across your entire infrastructure. The 405(d) HICP guide recommends that you include identity and access user controls, perimeter security, network security, patch management, intrusion prevention, and endpoint solutions. These are covered in more detail under their relevant practices in technical volumes 1 and 2.

How to use 405(d) HICP

When you're looking at building your organization's cybersecurity program, it's important to align that program to a national standard like the NIST Cybersecurity Framework. Section 405(d) does that mapping for you, based on organization size and resources.

But what else can you do? How can you put 405(d) HICP to build and mature your healthcare cybersecurity practices?

Here are five recommendations to help your organization adopt HICP Section 405(d):

1. **Establish a multi-year cybersecurity program strategic roadmap (requires current and desired state)**

In healthcare, staffing turnover is a real problem, especially right now. There's a lot of cybersecurity turnover, and it's challenging to attract and retain trained, skilled professionals. What can happen as a result is that some cybersecurity programs are built singularly off one person's experience or area of interest, so when that person leaves the organization, it can create a gap for your program. That's why it's important, instead, to draw on these industry-recognized best practices and develop a multi-year program with a strategic roadmap, one that takes into consideration your current security posture and how you want to mature your program over time.

After you've developed this roadmap, find a framework that helps get you where you want to go.

2. **Assess control performance against 405(d) HICP to identify priorities and milestones**

It's essential to identify your control performance using the 405(d) HICP framework. You want to go through each one of those practices and sub-practices to identify control status and identify your target profile.

You can look at control performance in several ways. It's not just control implementation but also control management, control definition, control reviews, and control updates. Review those in terms of the maturity model for each control.

Measure your policies and procedures defined around that and implement those controls. Also, you want to ensure those controls and control expectations are regularly reviewed and updated. In some cases, you even want to audit those controls. There is a maturity level scale related to these controls that can help you measure status within your organization.

3. **Establish annual tactical work plans, a cybersecurity oversight committee, and a program charter**

An oversight committee can help you implement your program, including building awareness, training, and communications policies and procedures as part of your strategic roadmap.

When creating annual tactical work plans, you can establish budget objectives to meet your strategic level goals or increase control capabilities within 405(d) HICP recommendations. A cybersecurity oversight committee is especially beneficial for medium and large healthcare organizations.

4. **Build consistency against your multi-year strategic roadmap and establish multi-year budgeting for activities**

Once you develop a multi-year strategic plan supported by annual tactical plans, you can do multi-year budgeting. This helps with control management and implementation.

If you're an organization heavily involved in mergers and acquisitions, you can consider the potential use of 405(d) HICP in this area.

5. **Continual performance, regardless of workforce member turnover (leadership, management, and subject matter experts)**

While those five steps are a great way to get 405(d) HICP in place and working for your organization, 405(d) HICP also has a lot of other practical uses you might not have considered, such as support for mergers and acquisitions, establishing vendor and supplier expectations, and strengthening relationships with your customers, investors, insurers, and regulators. Now, let's take a closer look at what that might look like:

Mergers and acquisitions support

Another way you can use 405(d) HICP is especially helpful if your organization is heavily involved in mergers and acquisitions (M&A). If you are heavily engaged in M&A, look at 405(d) HICP as a standard you measure and assess potential acquisitions.

For example, as part of acquisition due diligence, you can conduct a pre-acquisition assessment against these recommendations.

Here are a few ways to use 405(d) HICP during this process.

Establish acquisition due diligence based on 405(d) HICP. Remember, this framework maps to NIST CSF.

In this example, you might start with the 405(d) HICP guidelines for a small organization during due diligence and then post-acquisition move toward adopting and implementing the controls for medium and large organizations as the acquired entity integrates more into your environment.

You may also want to consider establishing portfolio-wide health care standards based on 405(d) HICP to assess and manage these standards. That's supported by 405(d) HICP, where controls are mapped to different capabilities. So, if you do a lot of healthcare portfolio work, adopting 405(d) HICP standards may be beneficial to support and enhance your processes.

Another way you may apply 405(d) HICP is as a resource to help your organization with assessment information, prioritizing investments, and controlling expectations. You can use it to prioritize your cybersecurity investments. When you look at those investments, it's critical to follow a proper investment workflow.

If your organization comes in and does a lot of assessment work, especially at high levels such as red team testing, you may not even have information system asset management; you may be throwing your money away. It may be better to invest in your program before doing advanced testing. You can use 405(d) HICP for guidance to help excellently prioritize those investments.

Vendor and supplier expectations

You can also use 405(d) HICP related to your vendor and supplier expectations. For example, you can build baseline standards based on 405(d) HICP for your vendors.

You can quickly point them to 405(d) HICP guidance, which they can use based on their organization size. You can explain that your organization is aligned with this program. You could consider starting all of your vendors with the 405(d) HICP standards for small vendors and then transitioning them as appropriate to standards for medium and large organizations.

You can use the same expectations internally as well. Then you'll be able to relate what your vendors look like to your own internal maturity status related to these controls.

Ultimately, it's important to remember that 405(d) HICP provides more specific guidance and controls than HIPAA. When you apply this guidance in addition to the law itself, you have much more solid regulatory grounding.

Customer and regulator communications

Another way you can use 405(d) HICP is related to your customer relationships, as well as those with your investors, insurers, and even regulators. Where these partners are interested in learning more about your cybersecurity practices, you can point them to 405(d) HICP and demonstrate that your practices are aligned to it and NIST CSF.

This is a good baseline when you're dealing with multiple stakeholders. You can explain that your program has a solid regulatory foundation. You can also demonstrate HHS alignment by, for example, sharing with your stakeholders some HHS materials related to 405(d) to highlight your program goals, objectives, and strategic alignment to mitigate the top threats healthcare faces today.

In addition, you can also highlight 405(d) HICP adoption within regulator and customer surveys or investigations. Many healthcare organizations receive surveys related to cybersecurity controls, especially business associates. You've got an excellent grounding if you've aligned your program to these standards.

Could insurance accept these standards one day? We know cybersecurity insurance providers are making many changes these days. A growing number of them require additional cybersecurity controls, such as multi-factor authentication and similar controls. They're constantly evaluating risks and threats, and early indications are that insurers are beginning to consider recognized security practices for assessing risk.

Reaping the benefits of 405(d) HICP

With 405(d) HICP and NIST CSF alignment, your healthcare organization now has a reliable set of standards based on organizational sizes with specific threats mapped to controls for your organization.

405(d) HICP is a great starting point for healthcare organizations looking to implement and mature their cybersecurity programs, but it's further strengthened by adopting the full NIST Cybersecurity Framework. While adopting the full standards will require more resources and time, doing so can elevate your security posture to a level that's more proactive and responsive to today's evolving and complex threat landscape.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact