



The Importance of Cyber Security as Critical Infrastructure to the Healthcare & Public Health (HPH) Sector

# FREQUENTLY ASKED QUESTIONS

On average, roughly \$6.35 million is lost due to data breaches in the healthcare industry; in the United States, this average raises to \$8.5 million worth of data breaches<sup>1</sup>. Small, medium and large organizations share the responsibility in protecting patient's vital data. The critical infrastructure community, the 405(d) initiative and the publication "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP), all work in tandem to create a culture of security and resiliency in the healthcare and public health sector further promoting that **Cyber Safety is Patient Safety**.

## What is Critical Infrastructure Security and Resilience Month?

*Critical Infrastructure Security and Resilience Month is an annual effort to educate and engage the private sector, all levels of government, and the American public about the vital role critical infrastructure plays to our Nation's well-being and why it is important to strengthen critical infrastructure security and resilience.*

As part of the Critical Infrastructure Security and Resilience Month, HHS' **405(d) initiative illustrates the critical relationship between the cybersecurity and the Health sector, with various publications and resources to help small, medium and large organizations to protect themselves from the growing threat of cyber attacks**. A more in depth look at critical infrastructure as a whole can be found on the Department of Homeland Security's (DHS) webpage dedicated to critical infrastructure as it relates to the healthcare and public health sector

## What is Critical Infrastructure and why is it important?

The Nation's **critical infrastructure provides the essential services that underpin American society**. Ensuring delivery of essential services and functions is important to sustaining the American way of life. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or a combination of any of these. They include the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; **healthcare and public health**; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems sectors. America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards and threats, both natural and man-made, including aging or failing infrastructure, extreme weather, cyberattacks, or evolving terrorism threats that impact our economy and communities. **Critical infrastructure security and resilience requires a clear understanding of the risks we face and a whole-of-community effort that involves partnership between public, private, and nonprofit sectors.**<sup>2</sup>



<sup>1</sup> Statistic retrieved from the "[Data Breach Calculator](#)" tool from IBM and the Ponemon Institute

<sup>2</sup> Definition retrieved from the Department of Homeland Security's National Protection & Programs Directorate 2018 [Toolkit](#)

## What is HICP and what is its purpose?

The main HICP document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. HICP identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. HICP also outlines a targeted set of applicable and voluntary practices that seek to cost-effectively reduce the cybersecurity risks of healthcare organizations.

**HICP was designed to strengthen the cybersecurity posture of the HPH Sector and help small practices and medium/large organizations prioritize what is important for their own protection. By using HICP, organizations can do their part to support the national health sector's cyber preparedness.**

The HICP publication aims to raise awareness and provide vetted cybersecurity practices to move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources.

## Is HICP a Federal Regulation?

**HICP is voluntary and is NOT federally mandated; it is not an expectation of minimum baseline practices to be implemented in all organizations.** It is a call to action to manage real cyber threats and is written for multiple audiences (clinicians, executives, and IT professionals) and is designed to account for organizational size and complexity (small, medium and large). The resource is more a reference to “get you started” while also bridging the gap of general knowledge of cybersecurity within the HPH sector. Following the publication is 100% voluntary, which is highly recommended to ensure your organization is using some of the best mitigation practices to protect your patients and your organizations. **HICP is also not a guide to HIPAA, GDPR, State Law, PCI or any other compliance framework.**

## What is 405(d) and how can I get involved?

The 405(d) effort is an HHS and industry-led public-private partnership to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH sector's cybersecurity posture against cyber threats. **The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.** For more information on this effort and to stay up to date on all 405(d) activities, please visit the 405(d) website at [www.phe.gov/405d](http://www.phe.gov/405d), or email us at [CISA405d@hhs.gov](mailto:CISA405d@hhs.gov).

## Why should I be worried about Cyber Attacks?

**Cybersecurity is a Shared Responsibility; a Team Effort.** It is not solely an IT issue; it is an enterprise issue with impacts to mission, business, and programs. For the health care industry, it is fundamentally about patient safety and uninterrupted care delivery. **HHS wants to do everything we can to help the health care community do what it does best – care for and protect patients.**

**Want More Information or Need to Obtain a Copy of the HICP Publication?**

Please visit the 405(d) website at [www.phe.gov/405d](http://www.phe.gov/405d) or email us at [CISA405d@hhs.gov](mailto:CISA405d@hhs.gov)