COSMOS
Navigate the Compliance Universe

Compliance Today - April 2024

Erika M. Riethmiller (erika.riethmiller@uchealth.org, linkedin.com/in/erika-riethmiller-33652656/) is the Chief Privacy Officer at UCHealth in Aurora, CO.

Recently published federal healthcare and public health sector-specific voluntary cybersecurity performance goals

by Erika M. Riethmiller

On December 6, 2023, the U.S. Department of Health and Human Services (HHS) released a*Healthcare Sector Cybersecurity* strategy paper.[1] This paper outlines HHS's goal to establish voluntary cybersecurity performance goals (CPGs) in alignment with the healthcare industry input, to enhance cybersecurity within the healthcare and public health (HPH) sectors. Since 2003, the federal government's Cybersecurity and Infrastructure Security Agency (CISA) Healthcare and Public Health Sector has been recognized by the federal government as one of 16 critical infrastructure sectors identified as being so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on national security and public health or safety. This paper was largely in response to the White House's March 2023 publication of its *National Cybersecurity Strategy* which outlined the administration's priorities regarding cyber resiliency in the U.S. by stating "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."[2]

The paper also built upon a July 2021 White House "National Security Memorandum Improving Cybersecurity for Critical Infrastructure Control Systems."[3] This memorandum outlined a series of actions that needed to be taken by the federal government to develop general (e.g., non-sector-specific) CPGs that would be consistent across all critical infrastructure sectors. CISA, in coordination with the National Institute of Standards and Technology (NIST), was tasked with developing these non-sector-specific CPGs. NIST is a nonregulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

On January 24—49 days after issuance of the strategy paper—HHS published the HPH CPGs along with a new "gateway website" designed to assist healthcare organizations in prioritizing implementation of the CPGs and easily access pertinent resources that could be used by organizations when implementing both the essential and enhanced CPGs.[4]

Why did HHS publish HPH CPGs so quickly?

First, the need was great. The HPH critical infrastructure sector has witnessed unparalleled increases in cyberattacks over the past decade. HHS's Office for Civil Rights (OCR) website—as described in the strategy paper—offers one glimpse into the explosion of cyberattacks against OCR-regulated healthcare entities, evidencing that from 2018 to 2022, there was a 278% increase in large breaches (breaches impacting over 500 individuals) reported to OCR that were the result of a ransomware cyberattack.[5]

Secondly, work to develop cyber-resilient resources for the healthcare sector, together with industry stakeholders, has been in place since 2015 when the Cybersecurity Information Sharing Act of 2015 (CSA)—a law designed to "improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats"—was passed into law.[6] This law made it easier for organizations to share personal information with the government in cases of cybersecurity threats, created a system for federal agencies to receive threat information from private organizations, and required that a task force be established to develop a document that "brought forth cybersecurity awareness and provided best practices for mitigating the most pertinent cyber issues within the healthcare sector."[7] CSA also established the 405(d) Program, which, later in 2017, resulted in the establishment of the 405(d) Task Group, a collaborative team of federal government and healthcare industry subject matter experts who have been hard at work since 2017 creating resources for healthcare organizations to enhance awareness of cyber risk and defend against cyberattacks.

To understand the impetus behind the HPH CPGs, it's important to look historically at recent federal cyber regulations and the federal government's players in the cybersecurity field.

- **CISA** – It works to protect the nation from cyber and physical threats and increase the cyber resilience of the nation's critical infrastructure.
- **HHS** – The federally designated Sector Risk Management Agency for the HPHs regarding cybersecurity. (Pursuant to the Homeland Security Act of 2002, as amended, and Presidential Policy Directive 21.)
- **Health Sector Coordinating Council (HSCC)** – A coalition of private-sector critical healthcare infrastructure entities organized to partner with and advise the federal government on identifying and mitigating strategic threats and vulnerabilities facing the sector's ability to provide services and assets to the public.
- **HSCC's Cybersecurity Working Group** – A group of more than 400 industry and government organizations collaborating to develop strategies to combat emerging and ongoing cybersecurity challenges to the health sector.