HHS releases voluntary cybersecurity guidance for health care organizations

January 10, 2019

The Department of Health and Human Services (HHS) estimates that U.S. health care systems lost around $6.2 billion in 2016 due to data breaches. Congress and HHS have recently taken affirmative steps towards reducing that amount.

Section 405(d) of the Cybersecurity Act of 2015 (CSA), titled "Aligning Health Care Industry Security Approaches," legislatively mandated the creation of the CSA 405(d) Task Group. That Task Group, comprised of over 150 health care and cybersecurity experts from government and industry partners, met in May 2017, to develop a set of voluntary, consensus-based principles and practices to improve cybersecurity in health care organizations of varying sizes.

The resulting publication includes four parts:

- Main Document, titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)" – Provides background and context related to cybersecurity threats in the health care industry and demonstrates the need for a coordinated set of industry-led guidelines, best practices and methodologies.
- Technical Volume 1 – Discusses ten cybersecurity practices and sub-practices for small health care organizations.
- Technical Volume 2 – Discusses ten cybersecurity practices and sub-practices for medium-sized and large health care organizations.
- Resources and Templates Volume – Provides additional resources and templates to supplement the other volumes.

Copyright © 2021 Bricker & Eckler LLP. All rights reserved.

The publication guides organizations on what to ask IT and/or IT security teams or vendors, but the technical volumes are meant for IT and/or IT security professionals themselves.

The five threats discussed in the HICP main document are:

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

The Technical Volumes explore the following ten practices to mitigate the identified threats:

- E-mail protection systems
- Endpoint protections systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

If you or your organization is interested in joining the 405(d) Task Group, HHS encourages you to reach out directly to the Task Group at CISA405d@hhs.gov.

Copyright © 2021 Bricker & Eckler LLP. All rights reserved.

Authors

Copyright © 2021 Bricker & Eckler LLP. All rights reserved.