Report on Patient Privacy Volume 23, Number 7. July 13, 2023
Security Checklist: Identifying Compliance Resources in Public, Private Sectors

By Jane Anderson

Health care entities seeking to address the seemingly myriad cybersecurity threats facing the industry should look outside their own organizations for help that's potentially available in two places: the federal government's growing health care cybersecurity resources and other health care entities.

Fortifying cyber defenses could be made easier by following guidance from government and public-private partnership advisory councils and working with other organizations—even if they are competitors—can help improve the cyber posture of the entire industry, security experts said recently.[1]

Erik Decker, vice president and chief information security officer at Intermountain Healthcare, chairs the Joint Cybersecurity Working Group for the Health Sector Coordination Council (HSCC), which partners with HHS and other federal agencies to develop strategic policy and operational approaches to prepare for, respond to and recover from significant cyber and physical threats. He recommended making use of three free resources released in the last four months, including:

- **HHS's Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,**[2] which outlines recommendations and best practices to prepare and fight against cybersecurity threats that can impact patient safety. HHS just released a new version of this guide, Decker said.

- **HHS's Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide,**[3] which also is available in a new edition.

- **HSCC's publication "Health Industry Cybersecurity – Managing Legacy Technology Security (HIC-MaLTS),"**[4] which Decker described as a comprehensive guide to managing cyber risk caused by legacy technologies used in health care.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login