Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Industry Publishes Recommended Cybersecurity Practices for Telehealth and Telemedicine

Washington, D.C., April 19, 2021- The Healthcare and Public Health Sector Coordinating Council (HSCC) today released a report with recommended security practices for how healthcare organizations, telehealth vendors and service providers should assess and mitigate potential cyber risks associated with the exponential increase in its usage. The document – "Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)" – is the 12th resource developed and published by the HSCC Cybersecurity Working Group (CWG) since 2019.

"HIC-STAT's publication is timely in light of the massive increase in the use of telehealth and telemedicine during the pandemic and the attendant increase in cybersecurity risks," said Mark Jarrett, Deputy Chief Medical Officer and Chief Quality Officer of Northwell Health in New York and the chair of the HSCC Task Group that produced the report. "This tool identifies potential cybersecurity risks in the use of telehealth and telemedicine and the regulatory underpinnings of its management, and provides recommendations for managing those risks," Jarrett said.

The HSCC CWG's executive director Greg Garcia said that "the audience for our resource is intended to be senior health provider executives with decision making authority over resource allocation and risk prioritization, senior IT security executives who can drive security policy through the enterprise, telehealth service and product companies, and regulators."

The HSCC encourages telehealth and telemedicine stakeholders to adopt the recommendations in HIC-STAT, as appropriate for their risk profile, and to urge others in their supply chain and constituencies to do the same to reduce risk to patients and their personal health information.

Other HSCC Joint Cybersecurity Working Group resources published since 2019 include:

- **Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2)**: The HIC-SCRiM v2 is a toolkit for small to mid-sized healthcare institutions to manage the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program.
- **Health Sector Return-to-Work (R2W) Guidance**: This guidance compiles recommendations and considerations for managing a return-to-work ("R2W") strategy for our healthcare institutions and companies approaching COVID phase-down, both domestically and internationally.
- **Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)**: The HIC-TCR is a tactical guide to advise health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency, such as the COVID-19 Pandemic.

- **Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)**:
  The HIC-PIC is a white paper with guidance for how healthcare organizations can protect trade secrets, medical research and other innovation capital from cyber theft.
- **Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)**:
  The HIC-ISBP is a best practice guide for how healthcare organizations can set up and manage cyber threat information sharing programs for their enterprise.
- **Management Checklist for Teleworking Surge During COVID-19 Response**:
  The Teleworking Management Checklist is designed as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and I.T. security, and supply chain resilience.
- **Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)**:
  The HIC-MISO identifies many of the cybersecurity information sharing organizations and their key services, as health organizations are beginning to understand the importance of cybersecurity information sharing and implementing information sharing systems.
- **Health Industry Cybersecurity Workforce Guide**:
  The HIC Workforce Guide is a tool kit for recruiting and retaining skilled cybersecurity workforce in the healthcare sector.
- **Health Industry Cybersecurity Practices (HICP)**:
  The HICP is a four-volume publication that seeks to raise awareness on managing cyberthreats and safeguarding patient safety for executives, health care practitioners, providers, and health delivery organizations, such as hospitals.
- **Medical Device and Health IT Joint Security Plan (JSP)**:
  The JSP is a total product lifecycle reference guide to developing, deploying and supporting cyber secure technology solutions in the health care environment.

About the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG). The HSCC is an industry-driven public private partnership of health companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 16 critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. The HSCC Joint Cybersecurity Working Group (JCWG) includes more than 300 health providers entities, medical device and health IT companies, plans and payers, labs, blood and pharmaceutical companies, and several government partners.

For more information: Greg Garcia, HSCC Cybersecurity Working Group Executive Director: Greg.Garcia@HealthSectorCouncil.org or visit us online at https://healthsectorcouncil.org

##