FACT SHEET

Healthcare Industry Cybersecurity (HCIC) Task Force

THE CHALLENGE

Over the past five years a dramatic escalation in cyber-attacks against the health care industry has put at risk personal privacy, financial security, health care research, and, most troublingly, patient safety.

MEETING THE CHALLENGE

The Cybersecurity Information Sharing Act of 2015, Section 405, required HHS to convene top subject matter experts from across industry and government to address this growing threat. The Health Care Industry Cybersecurity Task Force spent a year receiving and reviewing input from experts from inside and outside the health care industry and the general public in order to develop specific recommendations and best practices for a Congressional report that was released on June 2, 2017

The Task Force report demonstrates the urgency and complexity of the cybersecurity risks facing the health care industry and calls for a collaborative public and private sector campaign to protect our systems and patients from cyber threats. There are six (6) imperatives developed by the Task Force that forms the basis for the report. Each imperative includes a set of recommendations and associated action items for implementing the recommendation.

- **Imperative 1: "Define and streamline leadership, governance, and expectations for health care industry cybersecurity."**

  Recommendations within this imperative focus on leadership and accountability for cybersecurity in corporate governance structures, industry organizations, and government at all levels. The Task Force recommends the creation of a "cybersecurity leader" role within HHS to coordinate activities and serve as a single focal point for industry engagement across regulatory and voluntary cybersecurity programs.

- **Imperative 2: "Increase security and resilience of medical devices and health IT."**

  This imperative addresses the Cybersecurity Information Sharing Act's mandate to review the unique cybersecurity challenges of medical devices and electronic health records. This imperative takes a total product lifecycle approach, recommending a mix of regulatory, accreditation, information sharing, and voluntary development and adoption of standards to promote system security from product design and development through end of life.

- **Imperative 3: "Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities."**

  In this section, the Task Force outlines the major workforce challenges facing health care information technology and cybersecurity, especially among small, rural, and other lesser-resourced organizations. It recommends steps to enhance cybersecurity leadership in organizations, develop the nation's health care cybersecurity workforce, and create options for organizations to gain efficiencies by leveraging shared cybersecurity services.

- **Imperative 4: "Increase health care industry readiness through improved cybersecurity awareness and education."**

  This imperative focuses on increasing the cybersecurity posture within organizations by raising awareness among corporate leadership, educating employees on the importance of cybersecurity, and empowering patients to make better choices related to the security of their personal health information. The Task Force recommends that HHS work with government and industry partners to promote cybersecurity awareness across health care

Healthcare Industry Cybersecurity (HCIC) Task Force

- **Imperative 5: "Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure."**

  This section focuses on the significant problem of health care intellectual property theft related to areas such as clinical trials, drug and device development, big data applications, and general health care business operations. It recommends activities to increase the industry's understanding of the scope of the problem and the economic and other risks of continuing intellectual property loss.

- **Imperative 6: "Improve information sharing of industry threats, risks, and mitigations."**

  Recommendations under this imperative focus on the sharing of cyber threat information among government and industry stakeholders. The Task Force recommends general principles to follow in the establishment of cyber threat information sharing systems in health care, with a focus on ensuring that actionable information reaches small and rural organizations.

As called for by the Cybersecurity Information Sharing Act of 2015 the HHS Secretary has shared educational materials on cybersecurity, including the Task Force's report and appendix, with industry stakeholders to improve preparedness for and response to cybersecurity threats.