To: CHIME Members
From: CHIME Public Policy Staff
Date: January 2016
Re: Cybersecurity Act of 2015 – Sec. 405. Improving Cybersecurity in the Health Care Industry

Background: The Cybersecurity Act of 2015 was included in the Omnibus spending package that funds the federal government for Fiscal Year 2016. Iterations of cyber threat information sharing legislation passed both the House and Senate in 2015, and were merged into the final product included in the spending package.

Along with the broader provisions outlining the processes to share cyber threat indicators with the federal government and private sector entities, the Cybersecurity Act included language specific to improving the cybersecurity preparedness of the healthcare sector. A draft of the healthcare-specific language was first included in the Senate's Cybersecurity Information Sharing Act of 2015 when it passed in November (neither of the House-passed bills included health-specific directives), but the healthcare language was edited and ultimately included in the Omnibus spending package.

In 2015, CHIME requested Congress take the following actions relative to cybersecurity:

1. Congress should pursue legislative action to strengthen information-sharing networks across public and private stakeholders, with emphasis on healthcare;
2. Congress should encourage more investment in advanced cybersecurity and information risk management within healthcare through safe harbors or liability protection for those who participate in information sharing and risk management programs; and
3. Congress should pursue legislation that harmonizes other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines.

Summary of Major Provisions: Cybersecurity Act of 2015 – Sec. 405. Improving Cybersecurity in the Health Care Industry

Report to Congress –

1. Within a year of final passage, the Secretary shall submit a report to the Senate Health, Education, Labor & Pensions (HELP) Committee and the House Committee on Energy & Commerce on the preparedness of the Department of Health and Human Services and the healthcare industry stakeholders [as defined below] in responding to cybersecurity threats.
2. Contents of the report – with respect to the internal response of HHS to emerging cybersecurity threats
    a. A clear statement of the official within HHS to be responsible for leading and coordinating efforts of HHS regarding cybersecurity threats in the healthcare industry
    b. A plan from each relevant operating division and subdivision of HHS on how each will address cybersecurity threats in the healthcare industry, including a clear delineation of how each

division will divide responsibility among personnel and community with other division regarding efforts to address cyber threats.

Healthcare Industry Cybersecurity Task Force –

1. Within 90 days of enactment [March 17, 2016], the Secretary of HHS, with National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), shall convene healthcare industry stakeholders, cybersecurity experts, and any Federal agencies or entitles the Secretary deems appropriate to establish a task force to –
    a. Analyze how other industries have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;
    b. Analyze challenges and barriers private entities (excluding state and federal governments) in the healthcare industry face securing themselves against cyber attacks.
    c. Review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record (EHR)
    d. Provide HHS with information to disseminate to healthcare industry stakeholders of all sizes for purposes of improving their preparedness for and response to cybersecurity threats affecting the industry
    e. Establish a plan for implementing cyber threat information sharing SO THAT THE Federal Government and healthcare industry stakeholders may in real time share actionable cyber threat indicators and defensive measures
    f. Report to appropriate Congressional Committees on the findings and recommendations of the task force
2. The taskforce will dissolve one year after it is established.
3. Within 60 days of the task force termination, HHS shall distribute the recommendations to the healthcare industry to improve their preparedness and response to cybersecurity threats.

Aligning Healthcare Industry Security Approaches –

1. The Secretary of HHS shall establish through a collaborative process with DHS and NIST, and any other Federal entities and non-Federal entities a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures and processes that –
    a. Serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations
    b. Support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;
    c. Consistent with –
        i. Standards, guidelines, best practices, methodologies, procedures, and processes developed under the National Institute of Standards and Technology Act
        ii. Security and Privacy regulators promulgated under the Health Insurance Portability and Accountability Act of 1996
        iii. Provisions of the Health Information Technology for Economic and Clinical Health Act and amendments made by the Act;
        iv. Updated on a regular basis and applicable to a range of healthcare organizations.
2. Nothing in this section (the guidelines, best practices, etc) share be interpreted as granting HHS the authority to –

a. Provide audits to ensure that healthcare organizations are in compliance with the voluntary guidance
b. Mandate, direct or condition that the award of any Federal grant, contract or purchase, on compliance with voluntary guidelines

3. No Liability for Non Participation –
    a. Nothing in this section shall be construed to subject a healthcare industry stakeholder to liability for choosing not to engage in the voluntary activities authorized or guidelines develop under this section.

Incorporating Ongoing Activities – HHS may incorporate ongoing activities that are ongoing as of the day before the dated of enactments of this Act and that are consistent with the objectives of this section

Rule of Construction – Nothing in this section shall be construed to limit antitrust exemption or protected from liability.

Healthcare Industry Stakeholder –

a. Health plan, health care clearinghouse, or healthcare provider
b. Advocate for patients or consumers
c. Pharmacist
d. Developer or vendor of health information technology
e. Laboratory
f. Pharmaceutical or medical device manufacturer
g. Additional stakeholder as defined by HHS