OFFICE OF THE
CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN SERVICES

Fact Sheet: Cybersecurity Act of 2015, Section 405(d)

Aligning Health Care Industry Security Approaches

In 2015, the United States Congress passed the Cybersecurity Act of 2015 (CSA), and within this legislation is Section 405(d): Aligning Health Care Industry Security Approaches. As an approach to this requirement, in 2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 150 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts.

The Task Group's charge was to develop a document that is available to everyone at no cost and includes a common set of voluntary, consensus-based, and industry-led guidelines, practices, methodologies, procedures, and processes that serve as a resource to meet three core goals to:

1. Cost-effectively reduce cybersecurity risks for a range of health care organizations;
2. Support voluntary adoption and implementation; and
3. Ensure on an ongoing basis that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level.

Progress To-Date. The Task Group assembled in May 2017 and since then, many achievements have been made with this effort. The table highlights current accomplishments made by those involved.

Activity	Highlight of Accomplishment
Task Group	Produced and ratified a working draft of the first version of this document for pretesting; it is intended to "move the cybersecurity needle" across our diverse sector by identifying the five more salient threats facing the industry, and establishing ten cybersecurity practices to mitigate them. This shows HHS' commitment towards improving the security and resiliency of the healthcare community.
Pretesting	This summer, the 405(d) team traveled across the country to 7 cities. HHS acknowledges that addressing the threats to our sector requires a broad, collaborative approach across a multitude of organizations within government and the private sector.

Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health Sector

What is the 405(d) effort?

An industry-led process to develop consensus-based guidelines, practices, & methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats

How will 405(d) address HPS cybersecurity needs?

With a targeted set of applicable & voluntary guidance that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations

Who is participating?

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders

Why is HHS convening this effort?

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d)

Healthcare and Public Health (HPH) Sector Benefits

This joint HHS- and industry- developed document aims to increase awareness and foster consistency with cybersecurity practices for a wide range of stakeholders.

Sector Benefits

Aimed for use across varied audiences
Executives, Healthcare Practitioners, Information Security Professionals

Information sharing among differing cybersecurity maturity levels
Small, medium, and large healthcare organizations can vary in their level of cybersecurity maturity

Cybersecurity Awareness
It is critical for uninterrupted care delivery and patient safety

Enterprise Risk Management
Cybersecurity should be treated as an enterprise issue, not just an IT issue

The Document

The 405(d) document aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.

The document includes a **main document** and **two technical volumes**:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for small healthcare organizations
- *Technical Volume 2* discusses these ten cybersecurity practices for medium and large healthcare organizations.

The **5 current threats** identified in healthcare:

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Internal, Accidental or Intentional Data Loss
5. Attacks Against Connected Medical Devices That May Affect Patient Safety

The technical volumes discuss these **10 practices** in more detail, tailored to small, medium, and large organizations:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies