LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

# Cybersecurity at HHS: Driving Results through Collaboration & Risk Management

**Chris Wlaschin, Chief Information Security Officer**
**HHS Office of Information Security**

**March 6, 2018**

# Cybersecurity at HHS: Agenda

- The U.S. Department of Health of Human & Human Services: Who are we and what do we do?
- Healthcare and the Cyber World: What happens when the two mix?
- HHS Office of the Chief Information Officer Cybersecurity Program
- Improving Security Posture through Cyber Hygiene
- Risk Management: How to improve security posture through IT Modernization?
- Information sharing: What is HHS doing to help strengthen the security posture of the both HHS and the private health sector?
- Cyber Resiliency
- Closing and Q&A

# Cybersecurity at HHS: Objectives

Following this discussion, participants will be able to better understand:

- The scope of cybersecurity issues in the Healthcare and Public Health (HPH) sector
- HHS' mission and overall approach to managing cybersecurity risk
- Information sharing and collaboration efforts within the sector and the legislative drivers for such collaboration
- Opportunities for collaboration and partnership with HHS on cybersecurity

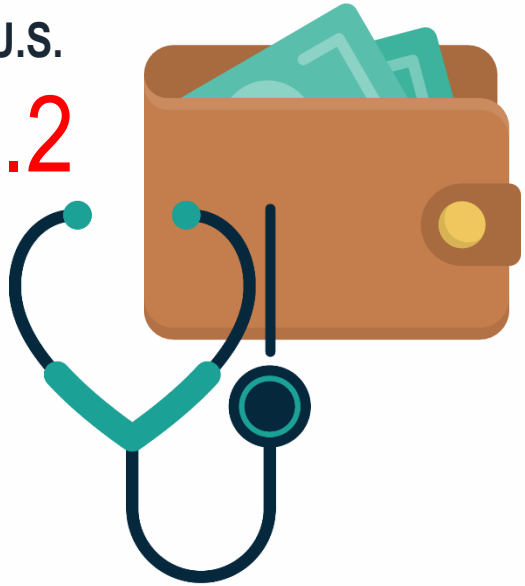
# U.S. Department of Health and Human Services

The U.S. Department of Health and Human Services: Improving the health, safety, and well-being of America.

HHS has over 79,000 employees working globally on a mission to enhance the health and well-being of Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.

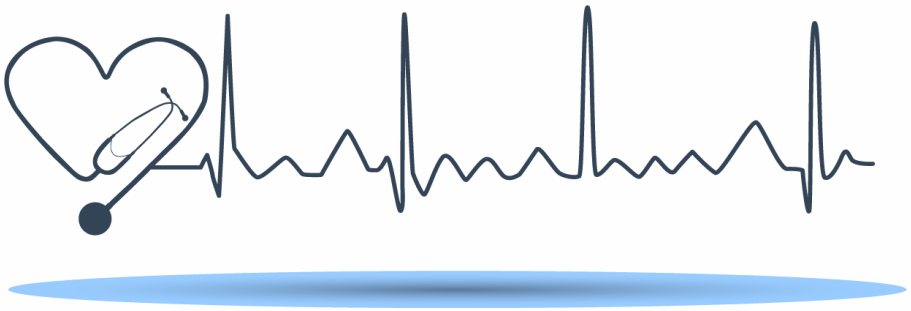
# Healthcare and the Cyber World

Data breaches cost the U.S. Healthcare system $6.2 billion in 2016.[1]



64% of physicians who experienced a cyberattack experienced up to four hours of downtime before they resumed operations.*

4 in 5 U.S. physicians have experienced some form of a cybersecurity attack.*

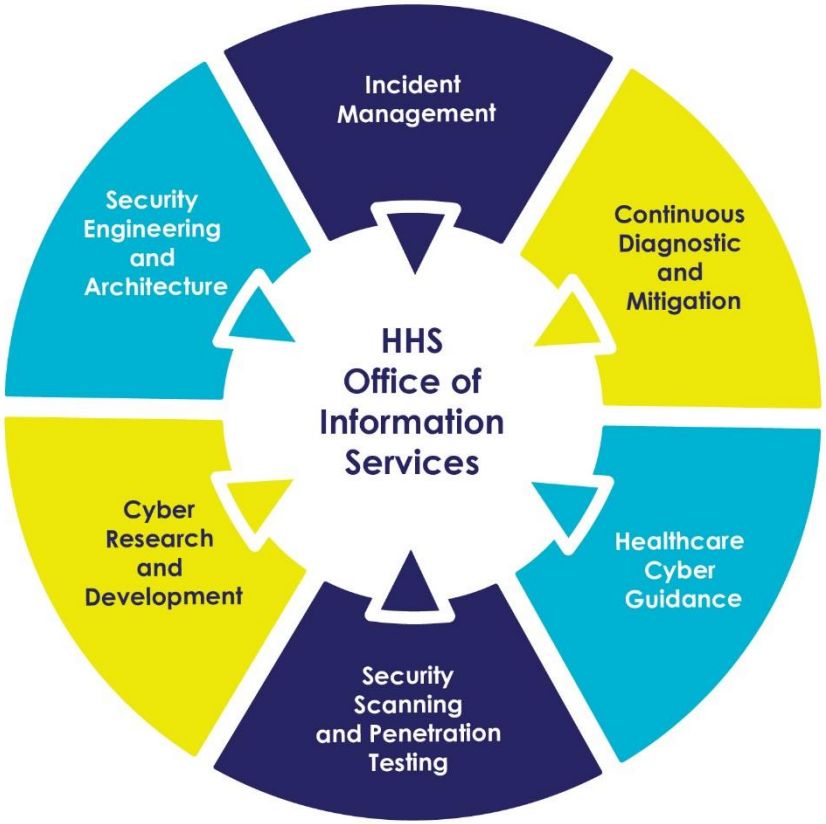


*2017 "Taking the Physicians Pulse" Study by the American Medical Association and Accenture [1]6 Ponemon 6th Annual Benchmark Study on Privacy & Security of Healthcare Data

# HHS OCIO Cybersecurity Program

The HHS Office of Information Security (OIS) is tasked with implementing a comprehensive, enterprise-wide cybersecurity program to protect the critical information with which the HHS is entrusted. To accomplish this, HHS provides and engages in:

- Implementing specific cybersecurity capabilities
- Cultivating cybersecurity partnerships in the public and private sectors
- Engaging in HHS-wide security collaboration activities
- Enhancing HHS' security capabilities through current and future programs and projects



# HHS Cybersecurity Protection

## Overview

**Healthcare Delivery**
80,000 patients in 34 states

**Finances**
$1M every minute in benefits 24/7/365

**Intellectual Property**
Medicine and medical devices

**Critical Research**
Open sharing of information world-wide

## Highlights

**2016**

9,047 cybersecurity incidents

Joint Federal Healthcare Threat Operation Center - 465 investigations & 14 identifiable threats

Biggest threats Phishing & Ransomware

**Last Month**

FDA 1.6+ billion security breach attempts

HHS investigated 5,226 incidents of spam; 450 malicious

HHS ran 600+ vulnerability scans on 120,000+ HHS web pages

**Operating Divisions**
Unique initiatives, focuses and capabilities
350 separate information systems
280,000+ hardware assets

**Committees**
Chair ISC²
HIMSS
CHIME

**2017 Budget**
$1.1 T
$12.6B for IT & $315.5M for Cybersecurity
2.5% of budget (average is 6-8%)

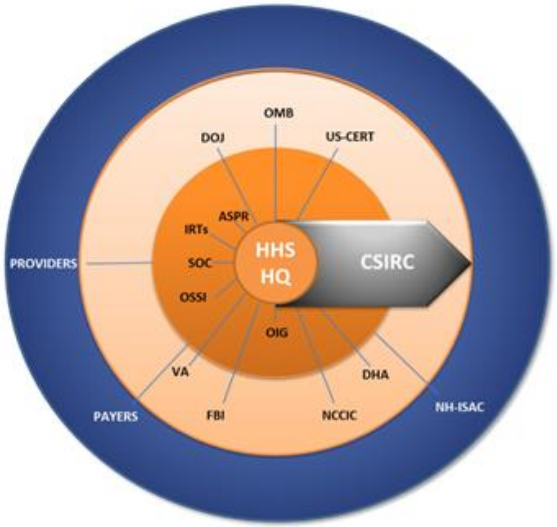
**Awards**

ISC² 2016 CISO– HIS

ISC² 2016 Best Cyber program – HHS CyberCare runner-up

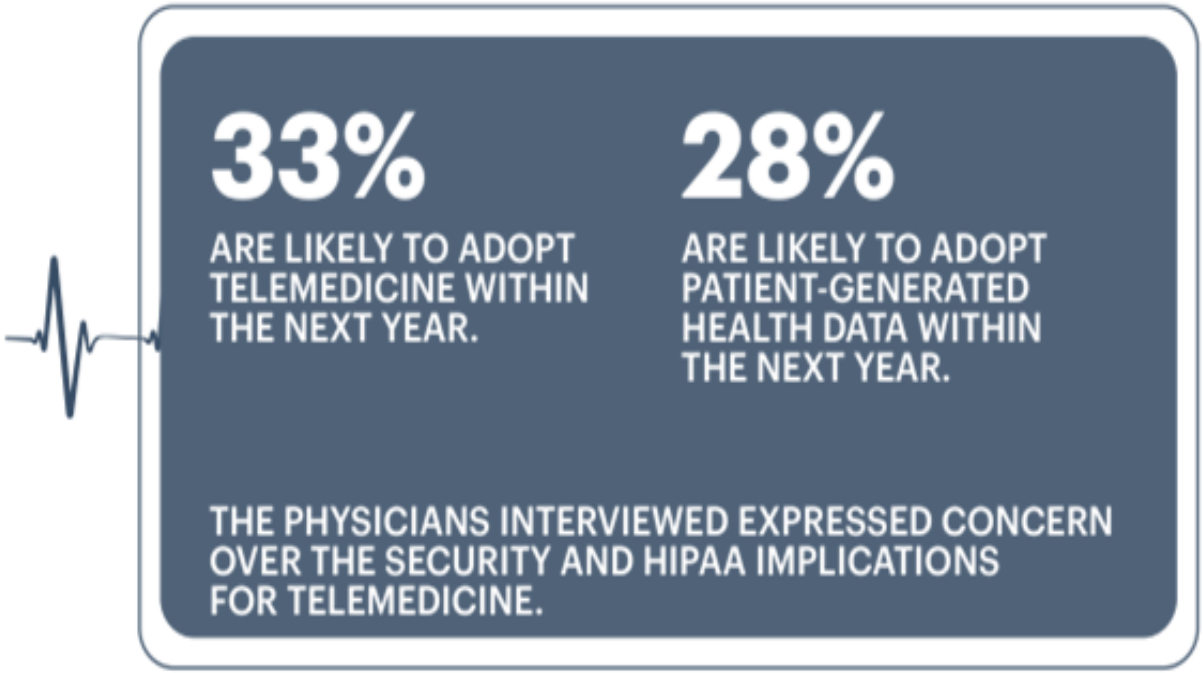
## Partners and Collaborators

Threat sharing information that is actionable and makes sense



# Risk Management and IT Modernization

**New technologies will bring many benefits but physicians must stay vigilant to new security challenges.**




*2017 “Taking the Physicians Pulse” Study by the American Medical Association and Accenture

# Risk Management & IT Modernization

- **Identifying High Value Assets (HVAs)**

  Through a enterprise risk management and priority risk management approach, HHS has identified and prioritized a list of High Value Assets that contain critical information.

- **Ongoing Authorization (OA) Program**

  A NIST mandated, time-driven or event-driven security authorization process with the goal of near real-time security state of the information system.

- **The Federal Risk & Authorization Management Program (FedRAMP)**

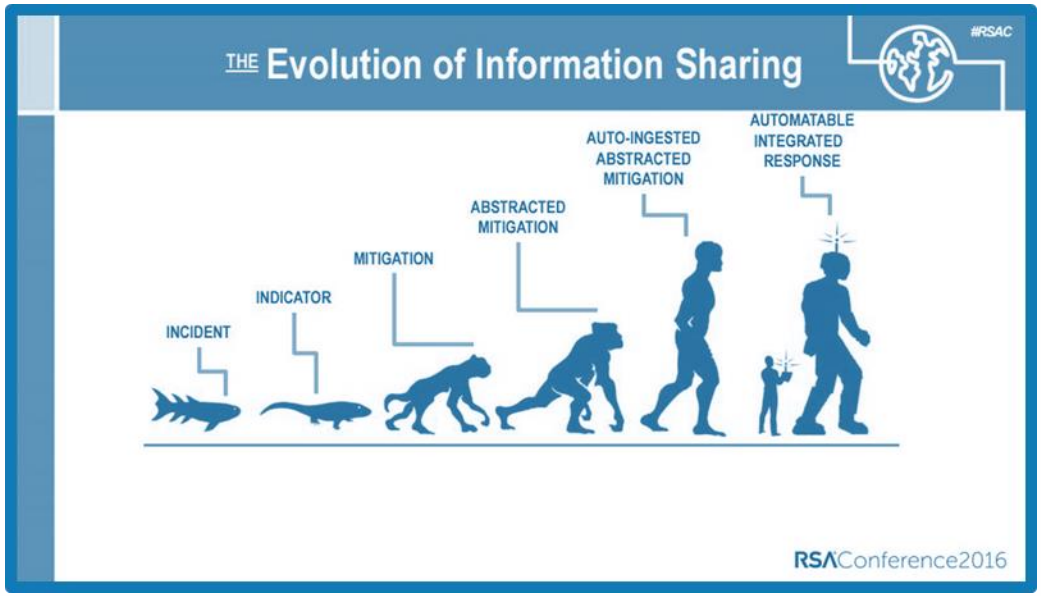
  A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

# Information Sharing

- Modernization and consolidation of networks
- Moving information to the cloud securely and keeping it safe
- Use of shared services to enable future network architectures
- Taking a risk based approach to legacy system modernization
- Mitigating discovered unsupported technology
- Collaboration within the Department and other organizations

# Information Sharing: Strength in Numbers

One of the first things we have to admit is that we cannot do it alone. It is only after collaboration with the public and private sectors, as well as the cyber community about vulnerabilities, threats being seen, communications, and other useful information do we start strengthening the security infrastructure and posture.



# Information Sharing: Strength in Numbers (cont.)

# Working as a Partner

## The Health Threat Operations Center (HTOC):

- The HTOC is a collaboration between HHS, the Department of Veterans Affairs (VA), and the Defense Health Agency (DHA) to share threat information among federal healthcare providing agencies

## The Computer Security Incident Response Center (CSIRC):

- CSIRC is the HHS centrally managed incident reporting function that works. On average 160+ incidents from across the Department are reported to the HHS CSIRC every week.
- CSIRC typically scans against all indicators of compromise (IOCs) – the unique fingerprints of an incident - immediately upon receipt and always within 24 hours.

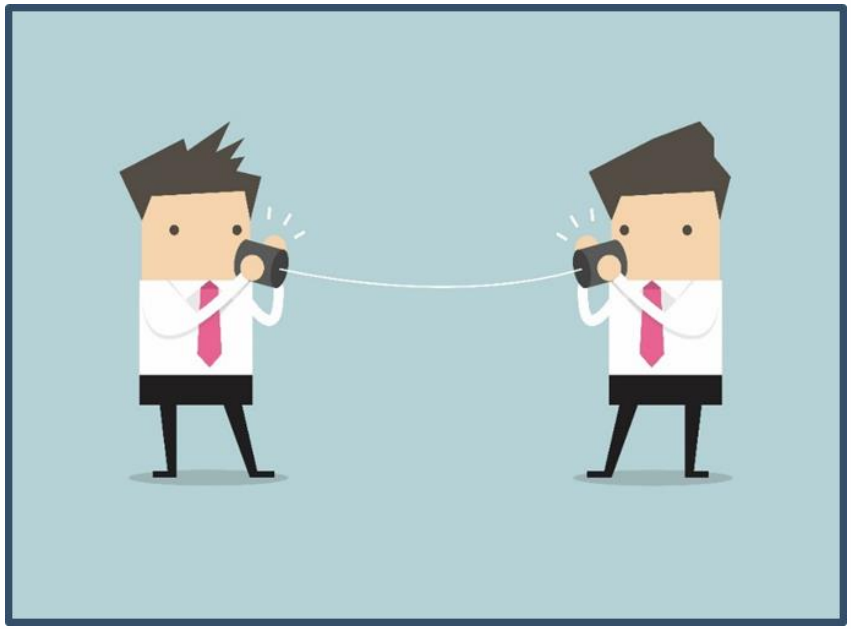
## Healthcare Cybersecurity Communications Integration Center (HCCIC)

- HHS builds trust by supporting both public and private health sector information security through the establishment and operation of the HCCIC.
- The HCCIC was an integral part of the coordinated response to the WannaCry incident. It provided analysis on the WannaCry threat and its impact on health care. HCCIC will strengthen engagement across HHS, increase awareness of healthcare cyber threats, and enhance public-private partnerships through regular engagement & outreach.

# Working as a Partner

## Cybersecurity Information Sharing Act (CISA)

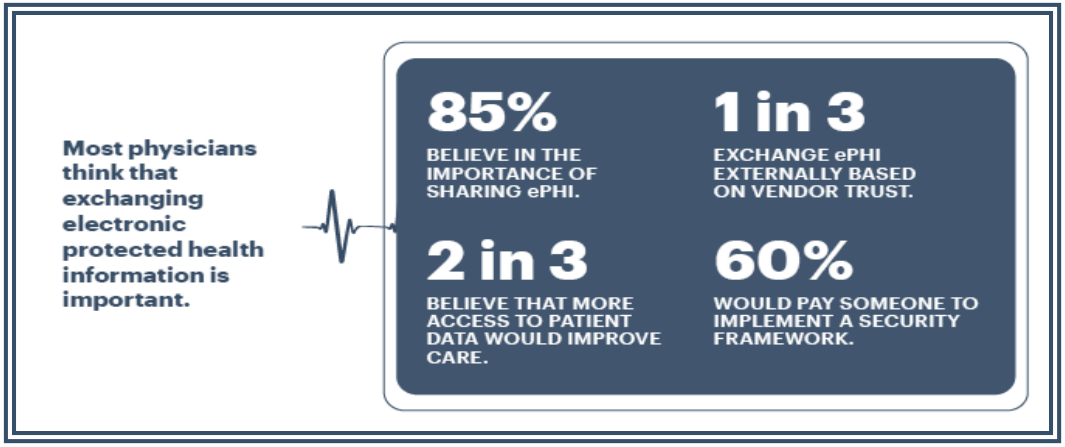
CISA is designed to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. CISA provides certain protections to encourage companies voluntarily to share information—specifically, information about “cyber threat indicators” and “defensive measures”—with the federal government, state and local governments, and other companies and private entities.



# Working as a Partner

## The Health Care Industry Cybersecurity Task Force:

- The Health Care Industry Cybersecurity Task Force received and reviewed input from experts from inside and outside the health care industry and the general public in order to develop specific recommendations and best practice to protect our systems and patients from cyber threats



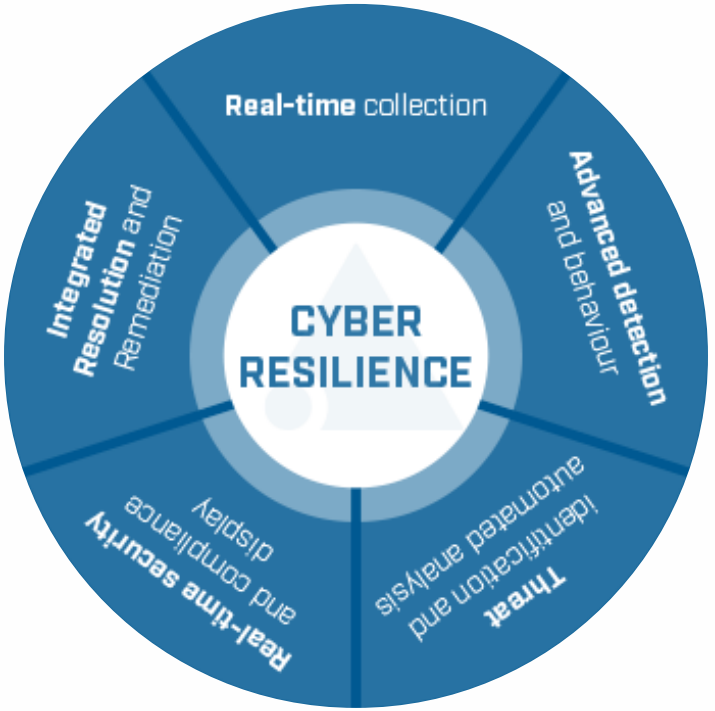

## Cybersecurity Information Sharing Act (CISA) 405(d):

- This is an industry-led process to develop consensus-based guidelines, best practices, and methodologies to strengthen the HPH-sector's cybersecurity posture.
- The goal is to create a targeted set of applicable and voluntary guidance that will cost-effectively reduce cybersecurity risks to a wide range of healthcare organizations.

# Cyber Resiliency

Keeping information secure, best practices in place, and having a business continuity plan leads to cyber resiliency. An organization's ability to be resilient in a world with constantly evolving cyber threats will:

- Keep data secure
- Keep people safe
- Avoid costly incidents



# 3 things you can do now to improve cyber hygiene

- Treat your patching report like your P&L Report
- Join an information sharing organization
- Get multifactor authentication for SA's and high profile people

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- **Automated Tools**
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

## Compensating Controls Include:

- Code of Conduct
- Security Training
- Phishing Training
- Automated Tools
- Segregation of Duty
- Detective Controls

# Closing and Q&A.