IROQUOIS *Healthcare Association*

Representing 54 hospitals and health systems in 32 counties of Upstate New York

CYBERSECURITY RESOURCES FOR HOSPITALS

Updated July, 2016

- **American Hospital Association**
  AHA cybersecurity page includes webcast and audio recordings.
- **National Institute of Standards and Technology**
  NIST Computer Security Resource Center provides information on federal standards and guidelines.
- **Healthcare Information and Management Systems Society**
  HIMMSS provides comprehensive privacy and security resources for health care providers.
- **HealthIT.gov**
  HHS HIT portal includes federal privacy and security standards and resources.
- **Medical Identity Theft FAQs for Health Care Providers**
  Information from the Federal Trade Commission to help health care providers minimize security risk and assist their patients if victimized.

ALERTS & BULLETINS

- **HITRUST Monthly Cyber Threat Briefing**
  The Health Information Trust Alliance, in partnership with HHS, provides monthly cyber threat briefings for healthcare organizations.
- **US-CERT National Cyber Awareness System**
  The U.S. Department of Homeland Security's Computer Emergency Readiness Team provides security information and updates including:
  - Current Activity High-impact types of security activity.
  - Alerts Security issues, vulnerabilities, and exploits.
  - Bulletins New vulnerabilities and patch information.
  - Tips General advice on common security issues.
- **HIMSS Healthcare Cybersecurity Reports** Monthly reports include information and resources for health care organizations on security threats, vulnerabilities and mitigation.

HEALTHCARE CYBERSECURITY NEWS

- **AHA News: Cybersecurity**
- **Healthcare IT News**
- **Health Data Management**
- **HHS ASPR Newsletter** June, 2016
- **HIMSS' Health IT Pulse**
- **Fierce Healthcare IT**

NATIONAL CYBERSECURITY FRAMEWORK & STANDARDS

- **NIST Cybersecurity Framework** 2013
  Presidential Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" directed development of standards and best practices to help organizations manage cybersecurity risks. Additional information is available on the NIST website.
- **Healthcare Sector Cybersecurity Implementation Guide** Updated May, 2016
  Health Information Trust Alliance guidance for implementation of NIST Cybersecurity Framework.
- **HIPAA Security Rule and NIST Cybersecurity Framework Crosswalk** February, 2016
  HHS released a crosswalk between the HIPAA Security Rule and NIST Cybersecurity Framework. "The security rule does not require use of the NIST Cybersecurity Framework, and use of the framework does not guarantee HIPAA compliance, the crosswalk provides an informative tool for entities to use to help them more comprehensively manage security risks" an HHS announcement stated. Related: HHS FAQ re: patents' rights to medical records and HIPPA Security Rule Guidance.

GUIDANCE

- **Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist** 2014
  Checklist issued by the Healthcare and Public Health (HPH) Sector Coordinating Council outlines cybersecurity items organizations should consider to protect their digital infrastructure.
- **Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101** 2014
  Developed by the Healthcare and Public Health (HPH) Sector Cybersecurity Working Group, the document addresses cybersecurity threats and recommended risk management activities.
- **Data Protection & Breach Readiness Guide** January, 2016
  The Online Trust Alliance provides resources including this guide for solutions for data protection.

MEDICAL DEVICE SECURITY

- **FDA Medical Device Cybersecurity**
  FDA recommendations for mitigating and managing cybersecurity threats.
- **Postmarket Management of Cybersecurity in Medical Devices** January, 2016
  The FDA issued draft guidance for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market. Related: FDA press release and AHA: Unique Cybersecurity Risks of Medical Devices.
- **Cybersecurity Vulnerabilities in Medical Devices** July, 2015
  Reviews factors contributing to cybersecurity vulnerabilities in medical devices and provides guidance regarding protection mechanisms, mitigations, and processes.

RISK ASSESSMENTS & INFORMATION EXCHANGE

- **Guide to Cyber Threat Information Sharing (Second Draft)** April 2016
  NIST guidance for healthcare systems on developing information sharing goals, identifying threat sources, engaging with existing information sharing communities, and effectively using threat information, which can help health systems share threat information in a structured fashion.

- **HHS Security Risk Assessment (SRA) Tool**
  The Security Risk Assessment tool was designed to help guide healthcare providers in small to medium-sized offices conduct risk assessments of their organizations' HIPPA compliance.
- **National Cybersecurity and Communications Integration Center (NCCIC)**
  The NCCIC within DHS provides situational awareness, incident response, information sharing and analysis programs and critical infrastructure protection.
- **U.S. Critical Infrastructure Cyber Community Voluntary Program**
  As part of Executive Order 13636, DHS launched the C3 Program to promote adoption of the NIST Cybersecurity Framework. The program includes:
  - Cyber Resilience Review (CRR) No-cost, voluntary, non-technical self-assessment or an on-site assessment of enterprise programs and practices.
  - Enhanced Cybersecurity Services (ECS) for Critical Infrastructure Entities Assists in protection of systems from unauthorized access, exploitation, or data exfiltration.
- **Cyber Security Evaluation Tool (CSET)**
  Developed through DHS National Cyber Security Division with assistance from NSIT, the software tool assists organizations in protecting key cyber assets.
- **InfraGard**
  An information and intelligence sharing partnership between the FBI and private sector.
- **National Health Information Sharing and Analysis Center (NH-ISAC)**
  NH-ISAC, a nonprofit organization responsible for the public and private health care sector's cybersecurity, has developed critical cyber threat and vulnerability sharing platform.
- **Hospital and Healthcare Information Breaches**
  HHS posts breaches of protected health information affecting 500 or more individuals.
- **The HITRUST Cyber Threat XChange (CTX)**
  Created to accelerate the detection and response to cyber threats targeted at the healthcare industry, CTX automates the process of collecting and analyzing cyber threats in formats that organizations of varying sizes and security maturity can utilize to improve cyber defenses.

INCIDENT REPORTING

- **US-CERT Incident Reporting System**
  Computer security incidents including phishing, malware, software vulnerabilities, and cyber threat indicators may be reported to US-CERT by completing a secure web-based form. For additional information about incident reporting, see US-CERT's Incident Notification Guidelines.
- **Federal Trade Commission – IdentityTheft.gov**
  Information on reporting and mitigating medical and other forms of identity theft.
- **Best Practices for Victim Response and Reporting of Cyber Incidents** April, 2015
  U.S. Department of Justice Cybersecurity Unit document provides planning and response guidance based on lessons learned through federal cyber investigations and prosecutions.

REPORTS & ANALYSIS

- **Health Care Cyberthreat Report** February, 2014
  The SANS Institute report examines how healthcare networks were attacked and provides recommendations for IT professionals and emergency planners.
- **State of Cybersecurity in Health Care Organizations** December, 2014
  A SANS Institute survey of health care organizations found 41% of respondents ranked data breach detection as ineffective and over 50% ranked the "negligent insider" as the primary security threat.
- **Hacking Hospitals** February, 2016
  An independent security firm issued a report of findings and recommendations from an assessment of hospital technology and cybersecurity. Its central theme is that "the healthcare industry focuses almost exclusively on the protection of patient health records, and rarely addresses threats to or the protection of patient health from a cyber threat perspective."

ARCHIVED WEBCASTS & RECORDINGS

- **Cybersecurity and Healthcare Facilities - HHS ASPR Webinar** June 6, 2016
- **Cybersecurity Risk Management and Response: Lessons for Health Care from Other Critical Infrastructure Sectors - AHA Webinar** June 9, 2016
- **What Health Care Leaders Need to Know to Adopt and Use NIST's Cybersecurity Framework - AHA Webinar** May 12, 2016
- **Cybersecurity Forum - HANYS Recorded Session** April 20, 2016
- **Ransomware - Emerging Cybersecurity Risk - AHA Audiocast** February 2016
- **Cybersecurity Education as a Tool for Risk Management and Reduction in Health Care Organizations - AHA Audiocast** February 2016
- **Cyber 911 - Responding to a Cybersecurity Breach - AHA Audiocast** December 2014