Introduction – Privacy, Security and Risk Management

What Healthcare Organizations Need to Know

HIMSS
transforming health through IT

Agenda

I. **Privacy, Security and Confidentiality**
   - Definitions in a Healthcare Context
   - Patient Privacy concerns
   - Security – CIA

II. **Today's Health IT Environment Creates Security Risk**

III. **Risk Management Concepts**

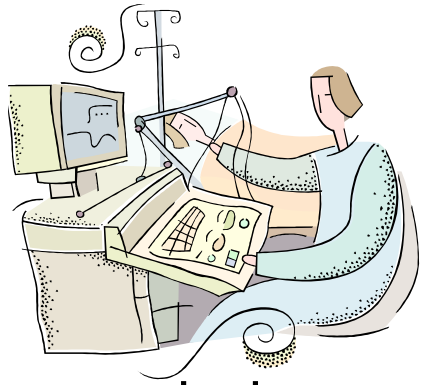
Privacy and Security Terminology
in a Healthcare Context

- **Health Information Privacy**
  - An individual's right to control the acquisition, uses or disclosures of their identifiable data
- **Security**
  - The physical, technical or administrative safeguards used to protect data from unwarranted access or disclosure
- **Confidentiality**
  - The obligation of those who receive the information to respect the privacy interests of those to whom the data relate
- **Use**
  - Within an organization
- **Disclosure**
  - Between/among independent organizations

HIMSS
transforming health through IT

Patient **P&S Concerns**

- Types of information collected
- How the information is handled internally
- Whether and how information is disclosed to external parties of any kind
- Children's privacy
- Security policies and procedures: physical and transmission
- Data mining/analysis policies
- User access to information
- The ability to correct information that was recorded in error
- Ability for privacy options to opt-in or opt-out
- How a site notifies users about any changes
- How to contact a site with questions



HIMSS transforming health through IT

AARP, "Personal Health Records: An Overview of What is Available to the Public"

Most Visible Privacy Policy Topics

- Confidentiality of Individual's Electronic Health Information
- Sharing of Individual's ePHI
  - Uses and Disclosures
- Secondary Uses of Health Data
  - Research, Marketing, Precision Medicine
- Data Ownership Model
  - Who "owns" the data?
- Security Breach Notification
  - Does the individual have the right to know that about a breach – that their privacy has been violated?

HIMSS
transforming health through IT

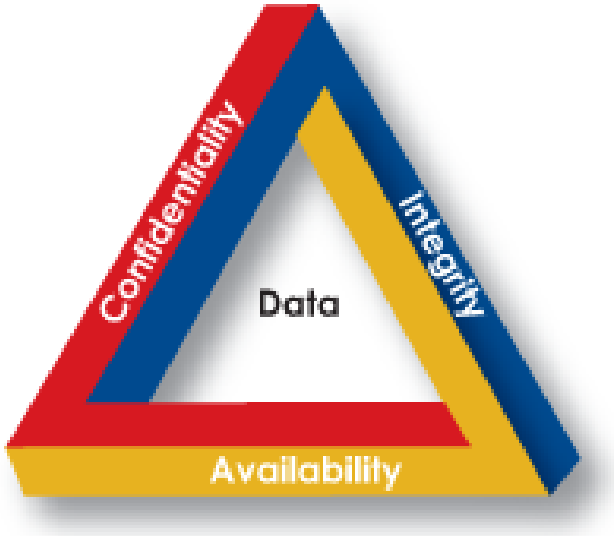
Healthcare's Use of IT Creates Security Risk

- Use of information technology has increased exponentially
- Information systems and networks now have nearly unlimited connectivity
- Medical Devices, monitoring devices and telehealth applications are all computer and internet enabled

HIMSS
transforming health through IT

Security - The CIA Triad

- Confidentiality
  - The information is not made available or disclosed to unauthorized individuals entities, or processes
- Integrity
  - Accuracy of the data must be maintained.
  - Data cannot be modified in an unauthorized or incorrect manner.
- Availability
  - The information must be available when needed.



Most often in Healthcare, we focus on…

- Confidentiality – Protect Patient's Privacy
  - The information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity
  - Accuracy of the data must be maintained.
  - Data cannot be modified in an unauthorized or incorrect manner.
- Availability
  - The information must be available when needed.

HIMSS
transforming health through IT

But, there are other aspects…

… *Patient Safety!*

- Confidentiality
  - The information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity
  - Accuracy of the data must be maintained.
  - Data cannot be modified in an unauthorized or incorrect manner.
- Availability
  - The information must be available when needed.

Today's Threats

- Increase in sophisticated threats and exponential growth rate in malware
- Cyber attacks are more organized, disciplined, and aggressive than ever before
- Today, adversaries are nation states, terrorist groups, and organized crime, and they are well funded and highly motivated

This results in an increasing number of penetrations of information systems in both the public and private sectors.

Threat Terminology

- Threat - the potential for a particular threat-source to successfully exercise a particular vulnerability.

- Vulnerability- a weakness that can be accidentally triggered or intentionally exploited.

"A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

* Source NIST SP 800-30 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Threat Terminology (continued)

- Threat-source - any circumstance or event with the potential to cause harm to an IT system.

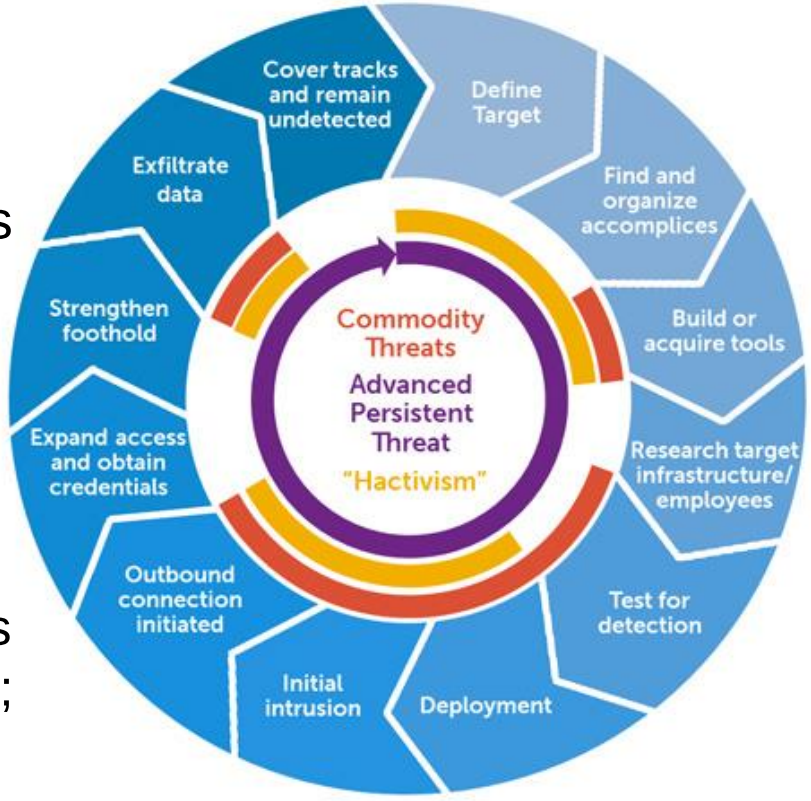
  Common threat sources can be *natural, human, or environmental.*

- Threat motivator - reason for or goal of action
- Threat actor – person, entity or program that executes

Advanced Persistent Threat

A threat actor that:

- Possesses significant expertise and resources
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, social engineering).
- Establishes footholds within IT infrastructure of targeted organizations:
  - To exfiltrate information;
  - To undermine / impede critical aspects of a mission, program, or organization; and
  - To position itself to carry out these objectives in the future.



HIMSS
transforming health through IT

Healthcare Organizations are Challenged to:

- Invest in New Technologies to Reduce Cyber Risk, for example,
  - Identity Management Solutions
  - Biometrics ,etc.
- Educate the Board of Directors & C-Suite about why Cybersecurity is a Business Priority
- Address the “Human Factor”: Insider Threats, Phishing Attacks, Mock Cyber/Phishing Exercises
- Upgrading Legacy Systems, Software, & Devices

Healthcare Organizations are Challenged to:

- Secure New Technology
  - Technology innovation may outpace data security innovation (for example, Mobile)
- Manage Product Life Cycles
  - Keeping Existing Software, Devices, & Systems Secure
  - Vendors Should Have a Mechanism for Updates & Fixes

Discussion

HIMSS
transforming health through IT