Mitigating Risk with Network Connected Devices – A Collaborative Enterprise Approach

Gail M. Zielinski, MSN, RN-BC, Director, Clinical Informatics

Clinical Excellence
Healthcare That Is Safe

Session Objectives

- Describe the contribution of the Nurse Informaticist in partnering collaboratively in the development of a “programmatic” approach and system infrastructure for software-enabled connected devices to ensure security and safety
- Identify the risks associated with the use of devices connected to the network that may compromise HIPAA security, privacy, and care delivery
- Describe methods to proactively drive accountability for safeguarding network connected devices that
  - results in positive outcomes
  - ensures patient safety through protected health information
- Share lessons learned and recommendations for practice

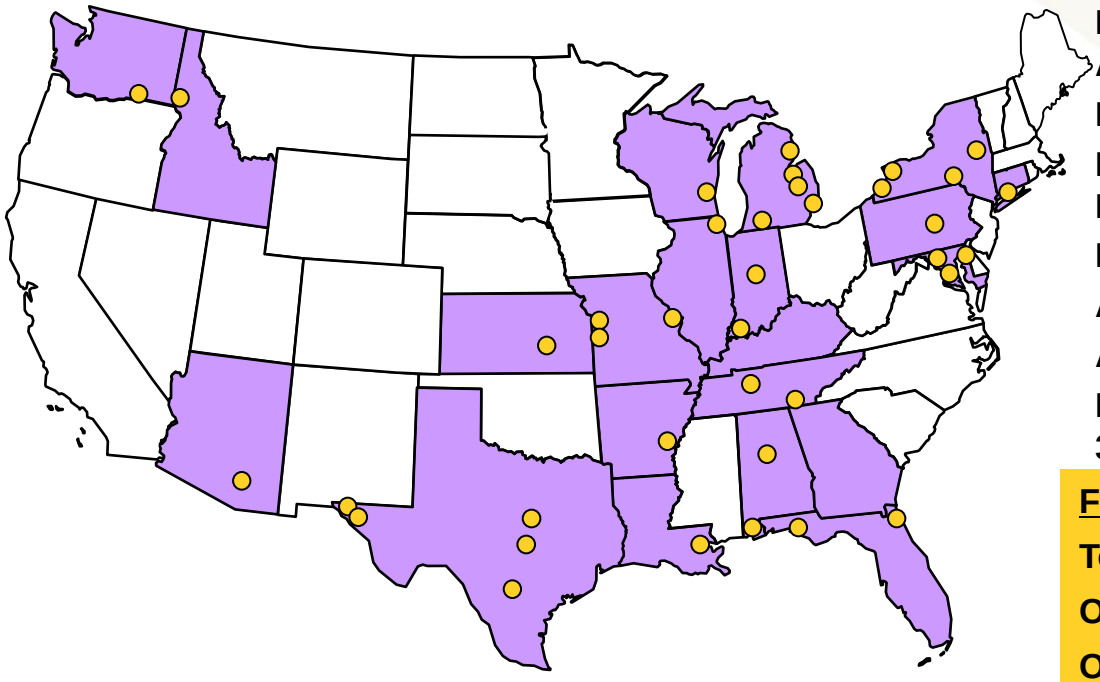
ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Ascension Health

We are the largest Catholic health system, the largest private nonprofit system and the third largest system (based on revenues) in the United States, operating in 21 states and the District of Columbia.

Care of Persons Living in Poverty and Community Benefit Programs $1.2 Billion*



Facilities and Staff

Locations	1,400
Acute Care Hospitals	70
Long-term Acute Care Hospitals	3
Rehabilitation Hospitals	2
Psychiatric Hospitals	6
Available Beds*	16,515
Associates	121,000
Physicians*	30,000

Financial Information (FY11)*

Total Assets	$20 Billion
Operating Revenue	$15.6 Billion
Operating Income	$424 Million
Net Income	$1.5 Billion

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

** Not inclusive of Alexian Brothers Health System*

What is at Risk to the Network?

- Can the following pose a risk to the network?
  - A copier/scanner **not connected** to the network
  - A digital video recorder (DVR)
  - USB devices that hold files or pictures

In the beginning….2009

Clinical Excellence
Healthcare That Is Safe

In the beginning…2009

- Increasing clinical device integration
- Estimated 10,000 network-connected medical devices
- 8 incidents within one year
  - MRI infected by a USB thumb drive
  - Interruption in patient care
  - Compromised patient safety

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

What should you know about Malware?

- Malicious software
  - Based on the perceived intent of the creator
  - Targets a computer's operating system
  - Potential results in data loss, confidentiality intrusion, etc
- "The release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications"*

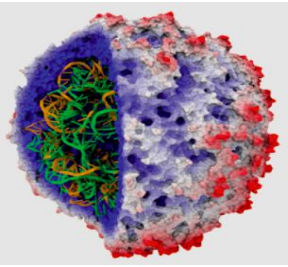
*published results from Symantec in 2008

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Computer Critter Categories

- Viruses



Security ‘holes’ (that require patching)

- Worms

Security breach in the OS, but do not act immediately

- Seeking other computers or programs to infect called ‘botnets’) awaiting instructions from each other, a host or other programs to activate themselves

Do not ‘kill the host Cornficker infects some 6.5M computers silently worldwide.

- Trojans

Hidden acceptable code, not requiring a ‘breach point’ because they are camouflaged

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Recognize Risks associated with Devices connected to the Network

- Devices containing Personal Health Information (PHI) may be subject to HIPAA security and privacy regulations
- Type of devices that are at risk include personal CDs, USB devices, and others
- Clinical or non-clinical computerized devices are often not protected by a malware defensive infrastructure
  - Potential for worms, viruses, Trojan horses, etc
  - If infected may require disassociating equipment and may impact the ability to provide care (e.g. CT scanner)
  - An existing malware intrusion detection system, which controls those technical assets deployed by a vendor partner and works under the supervision of the organization, must be in place

What is at risk? Software Containing Medical Devices (abbreviated):

- Anesthesia units
- Anesthesia ventilators
- **Apnea monitors (stimulator)**
- Argon enhanced coagulation units
- Aspirators
- Auto transfusion units
- **Cardiac defibrillator int./ext.**
- Electrosurgical units
- External pacemaker
- **Fetal monitors**
- Heart-lung machine
- Incubators
- **Smart Infusion pumps**
- **Invasive blood pressure units**
- **Pulse oximeter**
- Radiation-therapy machines Ventilator
- Physiologic monitors
- ECG
- EEG
- Treadmills
- Ultrasound sensors
- Phototherapy units
- Endoscopes
- Human-implantable RFID chips
- Surgical drill and saws
- Laparoscopic insufflators
- Phonocardiographs
- **Beds**
- Radiant warmers (adult)
- **Electronic thermometer**
- **Breast pumps**
- Surgical microscope
- Ultrasonic nebulizers
- Sphygmomanometers
- Surgical table
- Surgical lights
- Temperature monitor
- Aspirators
- X-ray diagnostic equipment
- Lensometer
- MRI control computers

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Industry Awareness - The big tickets……..

- Hundreds of devices not compliant with dozens of HIPAA statutes
- Fines are possible for each incident, at $10K per incident, could result in millions of dollars of expenditure and sanctions
- Malware leading to data loss, security breaches, operating malfunctions, confidentiality intrusion; unlawful, enforceable and expensive, safety issues notwithstanding

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Partnering Collaboratively: Development of a Programmatic Approach and System Infrastructure

Clinical Excellence
Healthcare That Is Safe

Collaborative Approach and System Infrastructure

- Senior Executive Council Task Force established in 2010 to investigate potential security risks resulting in the Connected Devices Program
- Clinical Informatics Executive Sponsor appointed
- Focus on an Ascension-wide program that supports the project strategy and becoming a High Reliability Organization
    - Solution Deployment
    - Continuing education to reinforce program concepts
    - Formalize ongoing operations of program methodology

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Connected Device Protection Program (CDPP)

- Early 2010
  - Launched System-wide Connected Device Protection Program
- Intent
  - Ensure that the medical and business computing devices that connect to Ascension Health's networks are protected
  - Mitigate our potential risk and resolve malware issues that can involve these devices

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Partnering Collaboratively

- Partner and establish a Core Team
  - Program Executive Leader
  - Clinical Infrastructure Director
  - Project Manager
  - Communications Manager
  - eProtex Director (ad hoc)

- Partner with Contracting and Legal
  - System level agreement focused on service expectations
- Partner with Executives
  - Quarterly Executive Meetings
  - Routine Communications

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Partnering Collaboratively

- Partner and establish a Multi-disciplinary Advisory Team
  - Strategy
  - Ascension Health University
  - Legal
  - Clinical Informatics (Nurse; Physician-CMIO)
  - Corporate Responsibility Officer
  - CHAN
  - Regional CIO
  - Regional Security Officer

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Contribution of the Nurse Informaticist

- Role of the Nurse Informaticist
  - Focus on impact to patient care and care delivery
  - Program management and oversee execution; co-manage budget
  - Serve as a liaison to Senior and local leadership, IS, eProtex
  - Facilitate messaging, conference calls, survey
  - Data analysis and program enhancements
- Develop a System Program and Methodology
  - Develop a System Level agreement focusing on service expectations inclusive of all Ascension Health inpatient hospitals
  - Address potential security risks with computer devices connected to the network that have ePHI and are not under security of the local data team
  - Conduct Market Analysis
  - Establish an Approach Document

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Implementation of a Programmatic Approach

Clinical Excellence
Healthcare That Is Safe

Work by eProtex

- Key Systems targeted for Safeguard Discovery
  - Clinical Systems and network servers that have ePHI
  - Wired, wireless, and interconnected systems
  - Point of Sale systems
  - Security and data security devices
  - Leased or vendor supported network devices
  - Devices not supported by Information Sxs
  - Pharmacy and medication security systems

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

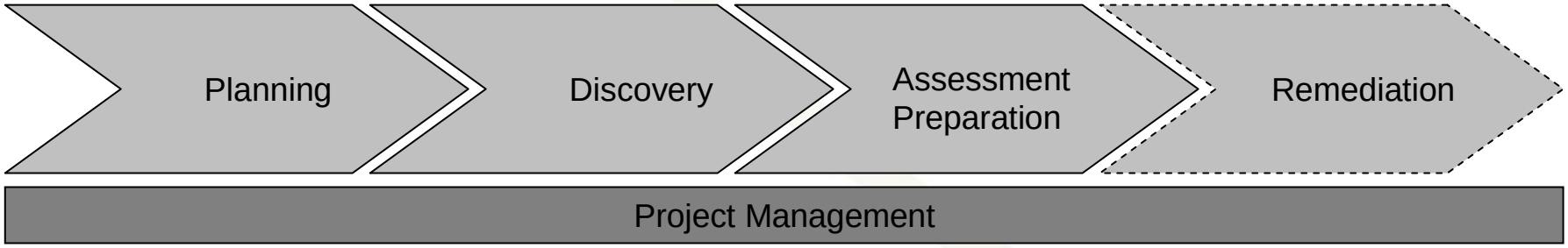
Operations: Deployment Approach & Schedule

- Standardized approach for Program deployment
  - Tools include a reference guide:
    - Program involvement and direction
    - Project level activities
      - Tasks
      - Timeline
      - Roles & Responsibilities
- System-wide deployment schedule
  - Local input “Health Ministry Champion”
  - Awareness of other large initiative coordination
  - Geographic location
  - Other synergies

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Deployment Project Overview



** Dotted line indicates the phase timeline is variable in relation to assessment findings and determined Hospital actions*

- The Safeguard Discovery deployment project at each hospital consists of three primary phases
  1. Planning: Engage the Hospital and eProtex team members for project kick-off
  2. Discovery: Catalog device inventory (on site)
  3. Assessment Preparation: Data analysis of device information and findings report generation
- Remediation is completed at the culmination of the Safeguard Discovery process to address identified device issues, which is variable by Hospital in relation to the findings during Discovery
- The process will be refined and enhanced across the deployment timeline

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Operations: Education/Communication Approach

- Identify target audiences and tailor communications to meet their needs
- Establish routine communications
  - Share findings and best practices utilizing various methods of communication including via the Web; use of discussion boards; etc
  - Count down communications (e.g. 60 days, 30 days, 2 weeks, 1 week)
- Various Methods for Education
  - Online tutorials
    - Access any time
    - Posted on our on-line learning platform
  - Online instructor-led training
  - Include examples for annual Corporate Responsibility Program

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Communications Plan "excerpt"

Topic, Tactic, Forum	Audience(s)	Frequency / Timing	File
Toolkit for AHIS Champion (60 Day Communication) • Memo from – project sponsor • Presentation – sent to AHIS champion to share with local leadership • Introduction memo – sent to AHIS champion to share with local AHIS team members inviting them to participate in program / attend kickoff meeting	AHIS staff at Health Ministry who will lead CDPP locally	Once – prior to kickoff meeting (around 60 days prior to inventory beginning)	Sample memo; presentation; introductory memo
30 Day Communication – Reminder of date for kickoff	AHIS staff at Health Ministry who will lead CDPP locally		

Operations: IS Procedures

- Established AHIS System-wide policies
  - Modified to address specific behaviors and vulnerabilities related to the Connected Clinical Devices Protection Program:
    - Third Party Connection and Devices
    - Computer Security Incident Responses

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Metrics and Outcomes

Metrics

- General Reporting total devices inventoried, compliant, at risk and level, remediation needs
- Source feedback from users via survey monkey
- Capture findings and look for trends within a network or equipment in different environments (e.g. video cam)
- Provide quarterly reporting to local and senior management

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Customer Satisfaction using survey monkey

General Questions	Yes	No	Comments
1. Did you receive sufficient information to be prepared for the eProtex data collection process?			
2. Do you know of any instance when data collection interfered with a clinician's work?			
3. Do you know of any instance when data collection interferred with patient care?			
4. The data collection personnel was considerate to the needs of the patients and employees (select one): Strongly agree; somewhat agree, neither agree nor disagree, somewhat disagree, or strongly disagree			
5. What could eProtex do better or differently next time?			

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Lesson Learned and Recommendations for Practice

Clinical Excellence
Healthcare That Is Safe

Lessons Learned

- Importance of enterprise programs comprised of an interdisciplinary team to drive positive outcomes and reduce costs
  - Ownership at the local level
  - Consistency and Resources
  - Advisory Council
- Appropriate budgeting
  - High/low
- Leadership engagement – reinforcement of scope
- Value of surveying and sharing experiences
  - http://www.surveymonkey.com/s/eProtex

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Program Scope and Revision

- 2010
  - 10,000 devices
  - .71 devices per bed
- 2011
  - Observed more than 2.1 devices per bed
  - Program suspended due to budget challenge
- 2012
  - Over 8000 devices inventoried to date
  - Re-estimate: 31,000 devices
  - 2.1 devices per bed
  - Contract amendment
  - New organization added
  - Program restart 7/10/12 for FY13

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

What is at Risk?

- True or False?
  - A copier/scanner **not connected** to the network can pose a risk (FALSE)
  - A digital video recorder (DVR) could be a source of risk to the network (TRUE)
  - USB devices that hold files or pictures are not a risk to the network (FALSE)

Think *before* doing!

Even the best security measures in the world can't bypass the problem of people not always thinking before doing.

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Q & A

References

- Federal Business Opportunities. (2011), OCR HIPAA Audit Protocol and Program Performance, Retrieved July 12, 2011 from http://www.fbo.gov
- U.S. Department of Health & Human Services. (2012), HHS settles HIPAA case with BCBST for 1.5 million, Retrieved March 13, 2011 from http://www.HHS.gov

ASCENSION HEALTH

CONNECTED DEVICES PROTECTION PROGRAM

Appendix: Market Research: Industry Sources*

*2010

- Manatt Healthcare
  - Engaged Managing Director and Senior Manager for industry research for connected device protection - removed specific names here and with other firms on slide
  - Manatt responded they had no research since this is such a new and emerging market
- Maryville Technologies
  - Engaged Vice President for educated industry advice for connected device protection
  - Mike responded with multiple providers that would fulfill a portion of the services that eProtex provides but none that singly matched all services

- Emergency Care Research Institute (ECRI)
- Gartner Research
  - Engaged Research Vice President Healthcare Provider to provide industry research for connected device protection
  - Gartner responded with the fact that eProtex has no peers with their breadth of service, multiple providers would have to provide similar service
- Forrester Research / KLAS
  - **Forrester** does not have available research in this industry segment
  - **KLAS** research on their website did not produce eProtex peers with similar breadth of service