MaineHealth

Cybersecurity in the Clinical Setting

Teri Young, MSB, RN-BC
VP & Chief Nursing Information Officer

November 9, 2017

Agenda

- Bridging the Gap Between Clinical and Technical
  - The Communication Challenge
  - Creating Shared Understanding
- Education and Awareness to Bridge the Gap
- Protecting Our Patients
  - Collaboration and Partnership
- Questions/Discussion

The Communication Challenge

- "It will only be a little while longer, we have this almost figured out…" *Network Engineer*
- "I can't access the system, what are we supposed to do? Do I use paper?" *Med/Surg Nurse*
- "We have to implement web proxy to better protect our systems, end users won't notice a thing" *IS Security Engineer*
- "I am waiting for this baby, why can't I get to Facebook?" *OB Provider*

Creating Shared Understanding

- Do your non-Clinical IS team members know what happens in the hospital, in the ambulatory setting, in the home health setting?
  - If not, they don't have a clear picture of what impacts happen when the system is not available

- Do your clinicians and support teams know what you 'do' in IS?
  - If not, they don't understand your challenging and 'unseen' work to keep things running and safe

- Common understanding is needed to support a united front to address cyberthreats
  - People need to know the 'why' behind the action

The Patient is ALWAYS at the Center

System Security Matters to Patient Safety!

- Recognized that data breaches have far reaching financial and privacy impact that can span years as the data is shared
- The loss of access to the EHR during a cyberattack impacts patient safety *immediately*
  - Many staff have never worked in a paper based record
  - Processes for managing paper orders/results for extended period of time are no longer in place (what did the unit secretary used to do?)
  - Access to historical information may be compromised

SAFER Guides

- The Office of the National Coordinator for Health Information Technology's SAFER (Safety Assurance Factors for EHR Resilience) Guides now include specific recommended practices for ransomware prevention

- **Organizational Responsibilities Guide**
  - Domain 1.4 "Organizations train all EHR users and IT staff on best practices related to maintaining patient privacy and data confidentiality while working with protected health information (PHI)."
    - » All employees required to take (and pass) course on protecting health information
    - » Train employees on ransomware prevention strategies (how to identify malicious emails, avoid clicking on potentially harmful attachments for example)
    - » Train employees not to use USB flash drives unless obtained from trusted source (like your IS Department!)

SAFER Guides

- **Contingency Planning Guide**

  - Domain 2.5 "Users are trained on ransomware prevention strategies including how to identify malicious emails."
    - » Education should include key elements of managing email (never download and run a file, never provide account or password information, etc)
    - » Restricting end user's ability to install and run software programs
    - » Consider disabling USB ports
    - » Conduct simulated phishing attacks to raise awareness

Education to Bridge the Gap - IS

- **Educate your IS teams about the use of the EHR by the clinical teams AND as importantly, what happens when they aren't available**
  - Interruption to patient flow when information is not easily available or easily updated, ex. making the next scheduled appointment
  - Increased length of time to do routine activities like medication administration
    # patients X # medications = less time for other patient care needs
  - Impact on other clinical areas such as lab where the techs have to manually complete specimen management from accessioning to resulting and reporting
  - Staff and Patient impact when the system returns as they enter hundreds of data elements back into the system to ensure that the patient story is complete

Education to Bridge the Gap - Clinical

- **Educate your clinical/support teams about the role that IS plays in keeping their systems running and SAFE**
  - Need to patch and update systems regularly to prevent untoward events
  - Reality that some of these activities may create planned interruptions in availability and why it is necessary
  - Do your end users know how many different people and skill sets it takes to keep things running?
    - » We are "IS" but do folks know what is beyond the Help Desk contacts they have?
  - Clinical users have The Joint Commission and CMS audits, do your end users know what audits are conducted in IS and why?

Partnering to Protect Our Patients

- Create a process where IS and key Clinical stakeholders (ex. Informatics teams, clinical managers, etc) can discuss and *plan* together for necessary system interruptions
- Create a Risk Assessment Checklist to assess clinical readiness for the system interruptions – secure sign off from all stakeholders on the agreed upon plan
- Perform post-event reviews with the key stakeholders
  - Lessons Learned opportunity
  - Educational opportunity for all parties
- All of this creates trust and mutual understanding

Our Responsibilities

- Clinicians have responsibility to keep patients safe from "cyber-harm"
  - Challenge people you don't know when they access computers on your unit – you wouldn't have let a stranger access a paper chart in years past!
  - Understand what phishing emails look like – you can 'open the door' to let the bad guys in…do you want to be known for that??
  - Are you saving PHI to places you shouldn't?
  - Is that your password posted next to the computer in the nurse's station?
- If your organization is attacked, you could be without your EHR for weeks. Think about what that will mean to your patient care practices…

Our Responsibilities

- IS – come out of hiding!
  - Make sure you introduce yourself and wear your badge, get to know users
  - Take the time to explain what you are there to do and why
  - Every opportunity is a teachable moment – don't waste it and remember to speak in layman's terms
  - Identify unit based educators, super users and charge nurses – educate them on safety techniques so they can help educate their co-workers
  - Consider using tools that simulate phishing to make the education 'real'

Collaborating to Win-Win

- Clinicians – partner with IS to look carefully at new systems or devices **before** purchasing, don't buy and *then* tell IS you have it and they need to implement
  - IS expertise is needed to ensure security requirements are met, confirm network capacity, assessment of the 'other' items that are needed to make it work – printers, scanner, network capacity
- IS – make it easy for Clinician/Operational Owners to plug into your expertise
  - Create a technology review committee that meets regularly and becomes a 'normal' part of the business case evaluation and provides a consistent avenue for clinicians to have their IS requests reviewed

Summary

- Clinicians are now gatekeepers in the protection against cyberthreats – help them to help you in IS in this work
- Create shared understanding among IS and Clinical stakeholders to reduce barriers and increase a united front in protection of our patients
- Use the 'evidence' such as SAFER Guides to formulate your plans – clinicians live in an evidence based world
- Make it easy to work together, reduce real and perceived barriers
- ***Remember that our patients are at the center of all we do!***

Questions/Discussion

Thank you!

References:

The Office of the National Coordinator for Health Information Technology's SAFER (Safety Assurance Factors for EHR Resilience) Guides:

https://www.healthit.gov/safer/sites/safer/files/guides/safer_organizational_responsibilities.pdf

https://www.healthit.gov/safer/sites/safer/files/guides/safer_contingency_planning.pdf