December 2017

Understanding the Risk & Challenges in Health IT

Eric Woo
Regional Director, Asia Pacific

ECRI Institute
The Discipline of Science. The Integrity of Independence.

©2017 ECRI INSTITUTE

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Medical Device Connectivity

- Health Information Technology (HIT) have created a strong push for **medical device data** to be **integrated with Hospital Information Systems** (HIS).
- The net result is the requirement for medical device integration. e.g.: between vital sign monitors and EHR, ventilators and physiologic monitoring system.
- Healthcare organizations are looking for medical device data to be more interoperable, complete, standardized, detailed, and accurate to improve clinical outcomes and patient safety.
- Interoperability allows different medical devices, information technology systems and software applications to **communicate, exchange data, and use the exchanged information** within and across organisational boundaries in order to advance the effective delivery of healthcare.
- Achieving interoperability can be difficult, as data format and encryption varies among vendors and models.

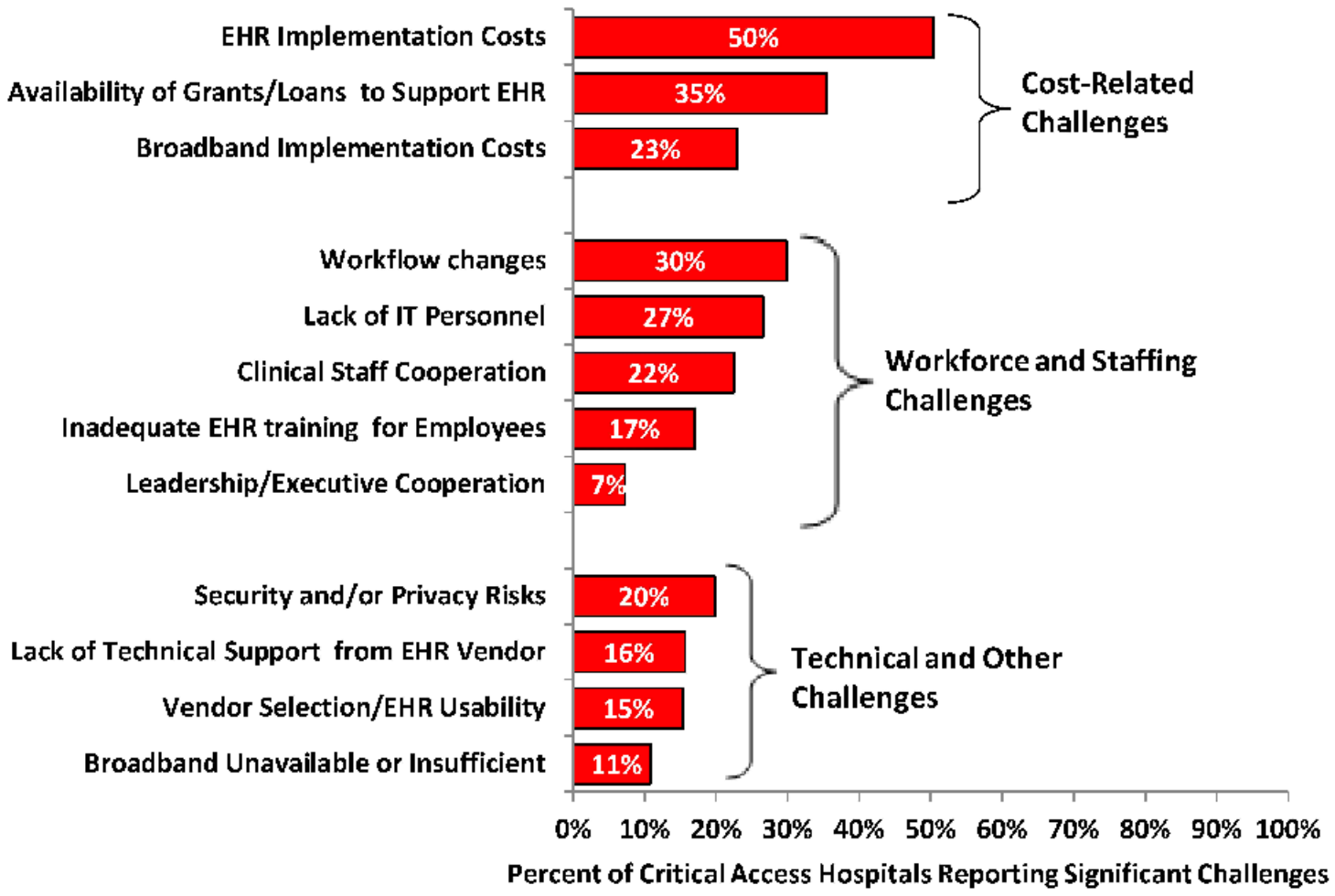
©2017 ECRI INSTITUTE

CHALLENGES OF HEALTH IT

©2017 ECRI INSTITUTE

Challenges of Health IT

Figure 3: Significant challenges to effective EHR implementation and use among Critical Access Hospitals.



SOURCE: ONC analysis of HIMSS Analytics 2013 CAH Survey Supplement

©2017 ECRI INSTITUTE

Risk - How do we know?

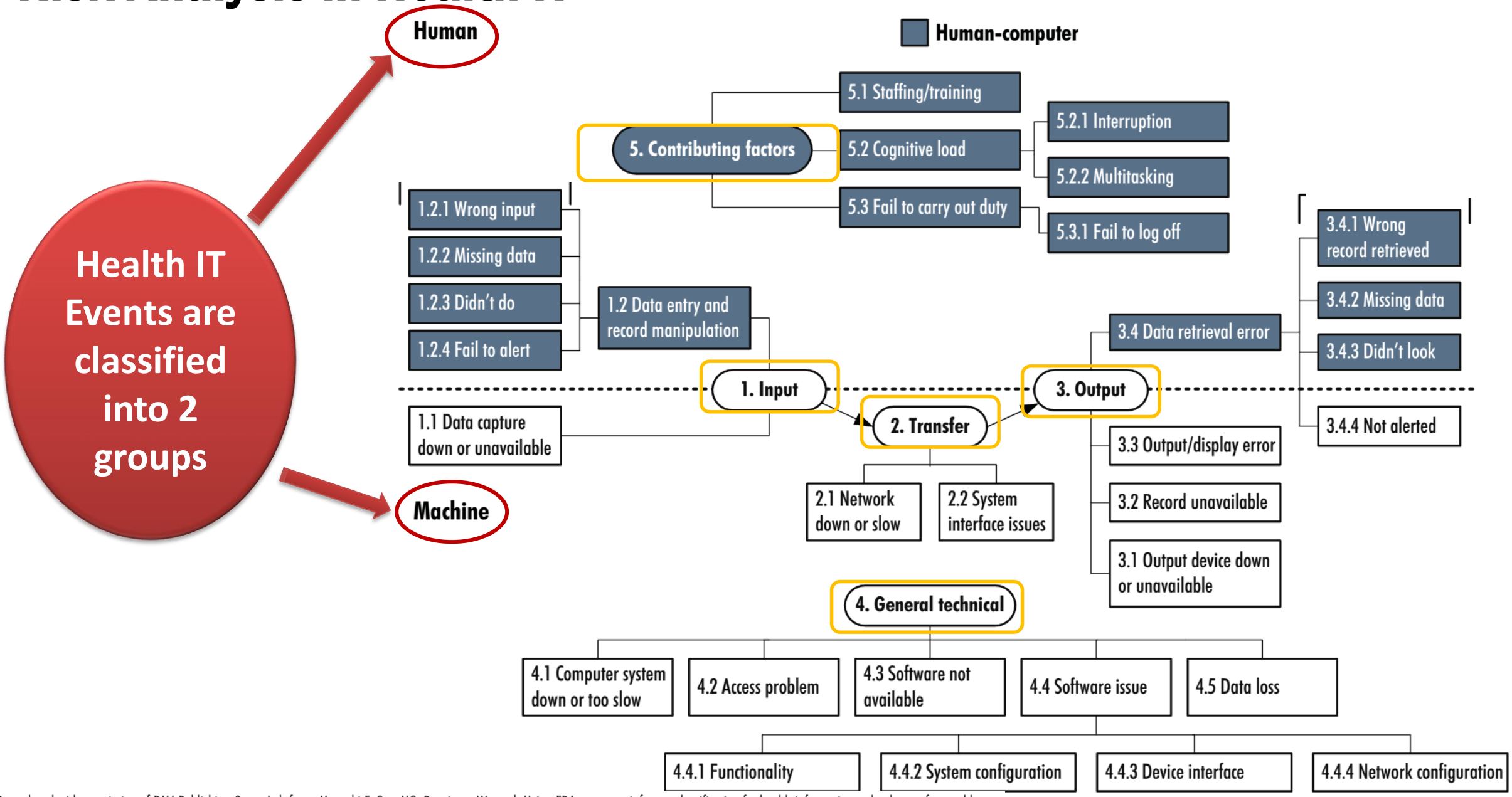
©2017 ECRI INSTITUTE

Risk Analysis in Health IT

- Health information technology (IT) provide multiple benefits to enhance patient care if the technology is ***optimally designed by the system developer, thoughtfully implemented by the healthcare organization, and appropriately used by the organization's staff.***
- However, Health IT can cause **"unintended adverse consequences"** if health IT system operates in unintended and unanticipated ways.
- Health IT-related incident can occur under the following circumstances:
  - The **system is unavailable** for use.
  - The system **malfunctions** during its use.
  - The system is **used incorrectly**.
  - The system **interacts incorrectly** with another and causes the loss of data or data being **incorrectly entered, displayed, or transmitted**.

©2017 ECRI INSTITUTE

Risk Analysis in Health IT



Reproduced with permission of BMJ Publishing Group Ltd. from: Magrabi F, Ong MS, Runciman W, et al. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012 Jan-Feb;19(1):45-53.

News Feature | April 29, 2014

Health IT Failure Top Hospital Concern

By Katie Wike, contributing writer

A recently released safety list from ECRI says failure of health IT systems should be the top concern for providers.

A new **report** based on research from the ECRI Institute lists top patient safety concerns for this year with health IT failures topping the list. ***iHealth Beat*** reports that the institute analyzed data from 1,200 hospitals on 400,000 patient safety events. Researchers then identified the top 20 patient safety concerns which experts narrowed down to a list of 10.

Question: Could this happen?

A) *The surgeon tried to access a patient's radiology study from the PACS system in the OR [operating room]. The display would only show a blue screen. The patient's time under anesthesia was extended while we tried to get the computer display to work.*

B) *The pharmacist entered medication orders, written and intended for one patient, for the incorrect patient. There is no system validation that the correct patient record is pulled up.*

C) *The wrong patient weight was manually entered in electronic record. The weight was entered as 75.5 kg instead of 175 kg, which could have affected any medication dosages given.*

©2017 ECRI INSTITUTE

RISK REDUCTION STRATEGIES

©2017 ECRI INSTITUTE

Risk Reduction Strategies : During Health IT Adoptions

Strength of Error-Reduction Strategies

Use special policies, procedures and education to reduce errors

Low Impact

- Document
- Educate or train
- Implement policies

Moderate Impact

- Simplify the process
- Standardize to reduce process variability
- Minimize choices
- Increase detectability
- Optimize redundancy

Do not eliminate hazards but use techniques to reduce the likehood of errors.
Highly dependent on user of system.

High Impact

- Automate
- Incorporate forcing functions
- Incorporate fail-safe mechanisms

Most powerful and desirable because it can eliminate hazards.

Organizations must consider a combination of the high-, medium-, and low-impact safety strategies to prevent any unintended consequences from health IT projects.
No one strategy by itself is effective in minimizing health IT-related errors.

Risk Reduction Strategies : The Process

The process:

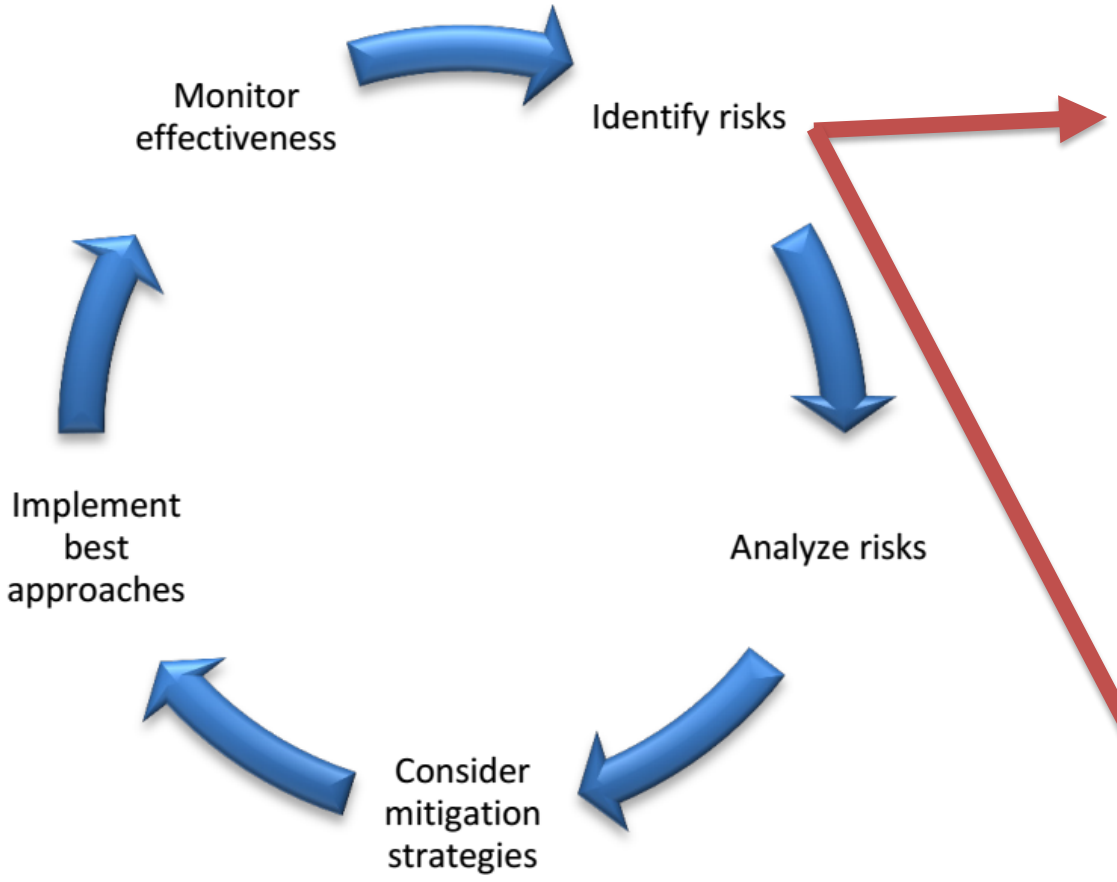
1. Who is involved?

- Clinicians, nurses, BME, IT, Risk Managers, vendors

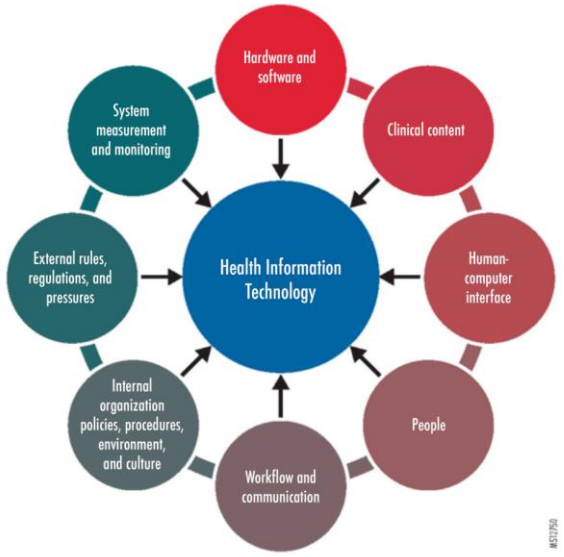
2. Why it is important?

- To identify HIT safety issues and prevent it from occurring (from first tested to implementation and operation)
- To design a process to capture the problems before patients are harmed

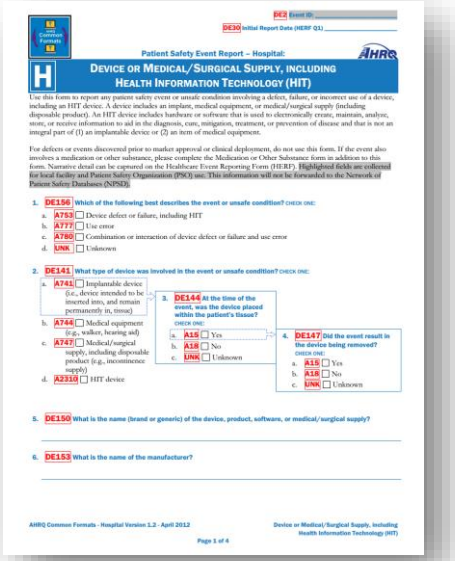
Continuous Feedback Approach to Health IT System Safety



A) 8 aspects for risk identification:



B) Event reporting tools:



Patient Safety Event Report – Hospital:

DEVICE OR MEDICAL/SURGICAL SUPPLY, INCLUDING HEALTH INFORMATION TECHNOLOGY (HIT)

Use this form to report any patient safety event or unsafe condition involving a defect, failure, or incorrect use of a device, including an HIT device. A device includes an implant, medical equipment, or medical/surgical supply (including disposable product). An HIT device includes hardware or software that is used to electronically create, maintain, analyze, store, or receive information to aid in the diagnosis, cure, mitigation, treatment, or prevention of disease and that is not an integral part of (1) an implantable device or (2) an item of medical equipment.

For defects or events discovered prior to market approval or clinical deployment, do not use this form. If the event also involves a medication or other substance, please complete the Medication or Other Substance form in addition to this form. Narrative detail can be captured on the Healthcare Event Reporting Form (HERF). Highlighted fields are collected for local facility and Patient Safety Organization (PSO) use. This information will not be forwarded to the Network of Patient Safety Databases (NPSD).

1. DE156 Which of the following best describes the event or unsafe condition? CHECK ONE:
   a. A753 ☐ Device defect or failure, including HIT
   b. A777 ☐ Use error
   c. A780 ☐ Combination or interaction of device defect or failure and use error
   d. UNK ☐ Unknown
2. DE141 What type of device was involved in the event or unsafe condition? CHECK ONE:
   a. A741 ☐ Implantable device (i.e., device intended to be inserted into, and remain permanently in, tissue)
      3. DE144 At the time of the event, was the device placed within the patient's tissue? CHECK ONE:
         a. A15 ☐ Yes
         b. A18 ☐ No
         c. UNK ☐ Unknown
      4. DE147 Did the event result in the device being removed? CHECK ONE:
         a. A15 ☐ Yes
         b. A18 ☐ No
         c. UNK ☐ Unknown
   b. A744 ☐ Medical equipment (e.g., walker, hearing aid)
   c. A747 ☐ Medical/surgical supply, including disposable product (e.g., incontinence supply)
   d. A2316 ☐ HIT device
5. DE150 What is the name (brand or generic) of the device, product, software, or medical/surgical supply?
6. DE153 What is the name of the manufacturer?

AHRQ Common Formats - Hospital Version 1.2 - April 2012 | Device or Medical/Surgical Supply, Including Health Information Technology (HIT) | Page 1 of 4

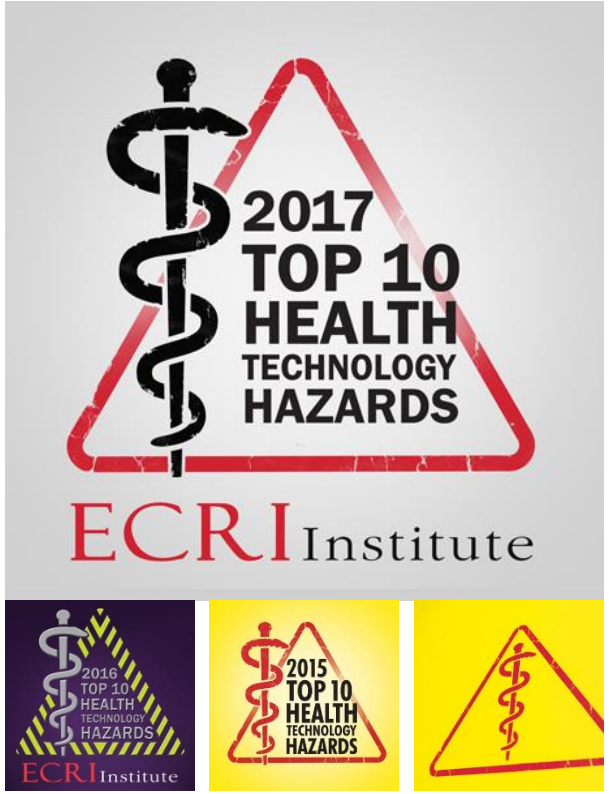
what's next?

ECRI Institute
The Discipline of Science. The Integrity of Independence.

©2017 ECRI INSTITUTE

Top 10 Health Technology Hazards - Cybersecurity

- 2017 - **#6.** Software Management Gaps Put Patients, and Patient Data, at Risk
- 2016 - **#10.** Misuse of USB Ports Can Cause Medical Devices to Malfunction
- 2015 - **#9.** Cybersecurity: Insufficient Protections for Medical Devices and Systems
- 2014 - **#7.** Neglecting Change Management for Networked Devices and Systems



©2017 ECRI INSTITUTE

Moving forward…

- Health Devices
  - Provide guidance to CE and IT in relation to medical device cybersecurity
  - Incorporating cybersecurity assessment in medical device evaluations
    - MDS2 form a standard request
    - Technology specific cybersecurity criteria
- BiomedicalBenchmark
  - Cybersecurity a part of standard IPMs
- Applied Solutions Group
  - Cybersecurity Gap Analysis
  - Medical Device Inventory Analysis

©2017 ECRI INSTITUTE

Privacy & Security

Hackers will target hospitals like never before in 2017

With Bitcoin allowing attackers to stay anonymous, and a bulls-eye painted over the industry, time to get prepared is running out, group says.

By **Tom Sullivan (/author/tom-sullivan)** | April 06, 2017 | 03:16 PM

17/04/2017 Hospital Returns to Pen and Paper After Virus Shuts Down IT Systems | Managed Care Magazine Online

Home News Current Issue Archives Original Research About

Hospital Returns to Pen and Paper After Virus Shuts Down IT Systems

Hackers believed to be involved

April 13, 2017

A virus succeeded in shutting down the entire computer network at the Erie County
t did not affect the
g to an article in the

illed prescriptions,
mputer systems back

Hospital pays ransomware, but doesn't get files decrypted

By Ryan Whitwam (https://www.extremetech.com/author/rwhitwam) on May 25, 2016 at 4:46 pm

35 Comments (https://www.extremetech.com/extreme/229162-hospital-pays-ransc
decrypted#disqus_thread)

392 shares

Topic

CYBERSECURITY NEWS

Cybersecurity Attacks Hit 87% of Organizations in 2016

A recent report found the majority of IT professionals said their entity was affected by a cybersecurity attack in 2016, with half expecting to raise their security budgets.

April 12, 2017 - A majority of organizations reported that they were affected by a cybersecurity attack last year, with one in three saying that they had been hacked more than five times in the past 12 months, **according to a recent Bitglass report (http://finance.yahoo.com/news/bitglass-report-87-percent-organizations-120000940.html).**

©2017 ECRI INSTITUTE

Privacy & Security

FDA gives Abbott 15 days to fix cybersecurity vulnerabilities in St. Jude Medical devices

by *Evan Sweeney* | Apr 14, 2017 12:00pm

The FDA warned Abbott that it needs to fix the cybersecurity concerns associated with its cardiac devices or face further penalties.

Those penalties could come at the expense of any Abbott devices that are in the FDA approval pipeline.

In a letter issued this week to Mike Rousseau, president of Abbott's cardiovascular and neuromodulation division, the FDA said the manufacturer failed to adequately address the cybersecurity concerns associated with its Merlin@home cardiac device, originally manufactured by St. Jude Medical.

Abbott acquired St. Jude Medical in January, but during an inspection in the following month, the FDA determined that Abbott had not implemented all of the corrective actions designed to mitigate cybersecurity risks and failed to confirm that any changes adversely impacted the device.

The FDA gave Abbott 15 business days to resolve the corrective actions and explain how it plans to prevent future violations.

©2017 ECRI INSTITUTE

©2017 ECRI INSTITUTE

What about IoT Impact?

- Data
- Communication
- Research
- Early diagnosis
- Monitoring
- Technological efficacy

Evaluation of Risk and Safety

ECRI Institute
The Discipline of Science. The Integrity of Independence.

©2017 ECRI INSTITUTE

Questions?

Eric Woo
Regional Director, ECRI Institute

Email: ewoo@ecri.org
Website: www.ecri.org

Thank You

ECRI Institute
The Discipline of Science. The Integrity of Independence.

©2017 ECRI INSTITUTE