National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

HIMSS 18 – FH06: Creating Practical Cybersecurity Guidance for PACS

March 6, 2018

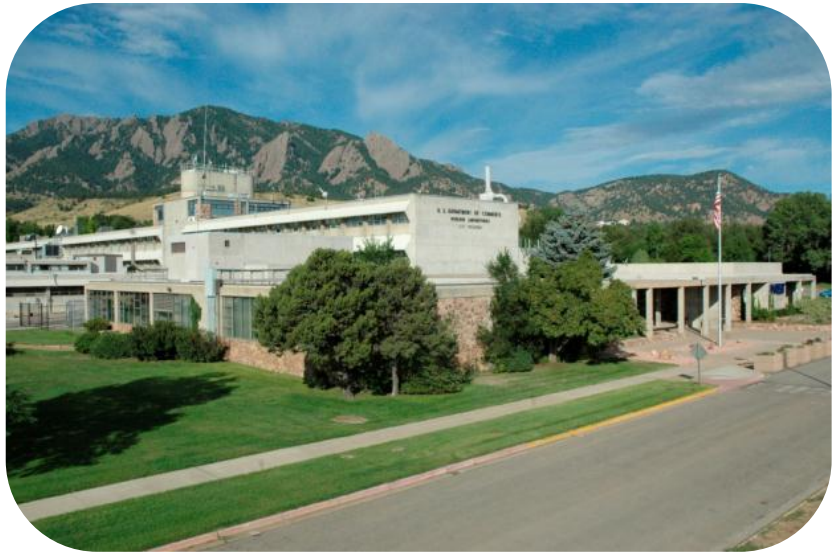
NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is where Nobel Prize-winning science meets real-world engineering.

Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing



With an extremely broad research portfolio, world-class facilities, national networks, and an international reach, NIST works to support industry innovation – our central mission.

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

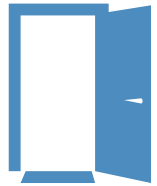
Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

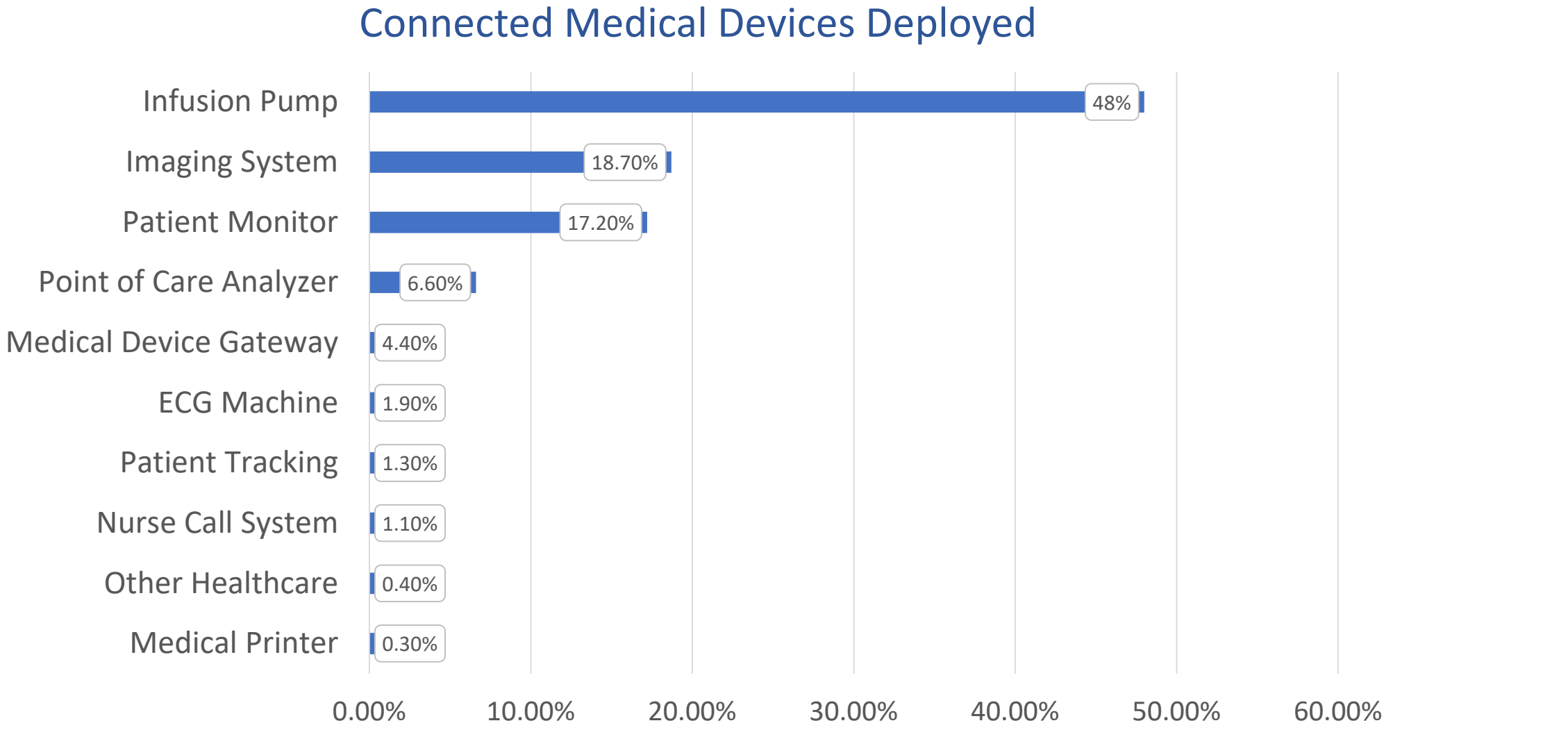
Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Function	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001:2013
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)	A.8.1.1, A.8.1.2
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(E)	A.8.2.1
PROTECT (PR)	PR.DS-1: Data-at-rest is protected	SC-28	IGAU, STCF	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)	A.8.2.3
	PR.DS-2: Data-in-transit is protected	SC-8	IGAU, TXCF	C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
DETECT (DE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4	AUTH, CNFS	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)	none
	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	AUTH, CNFS, EMRG, MLDP	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)	none

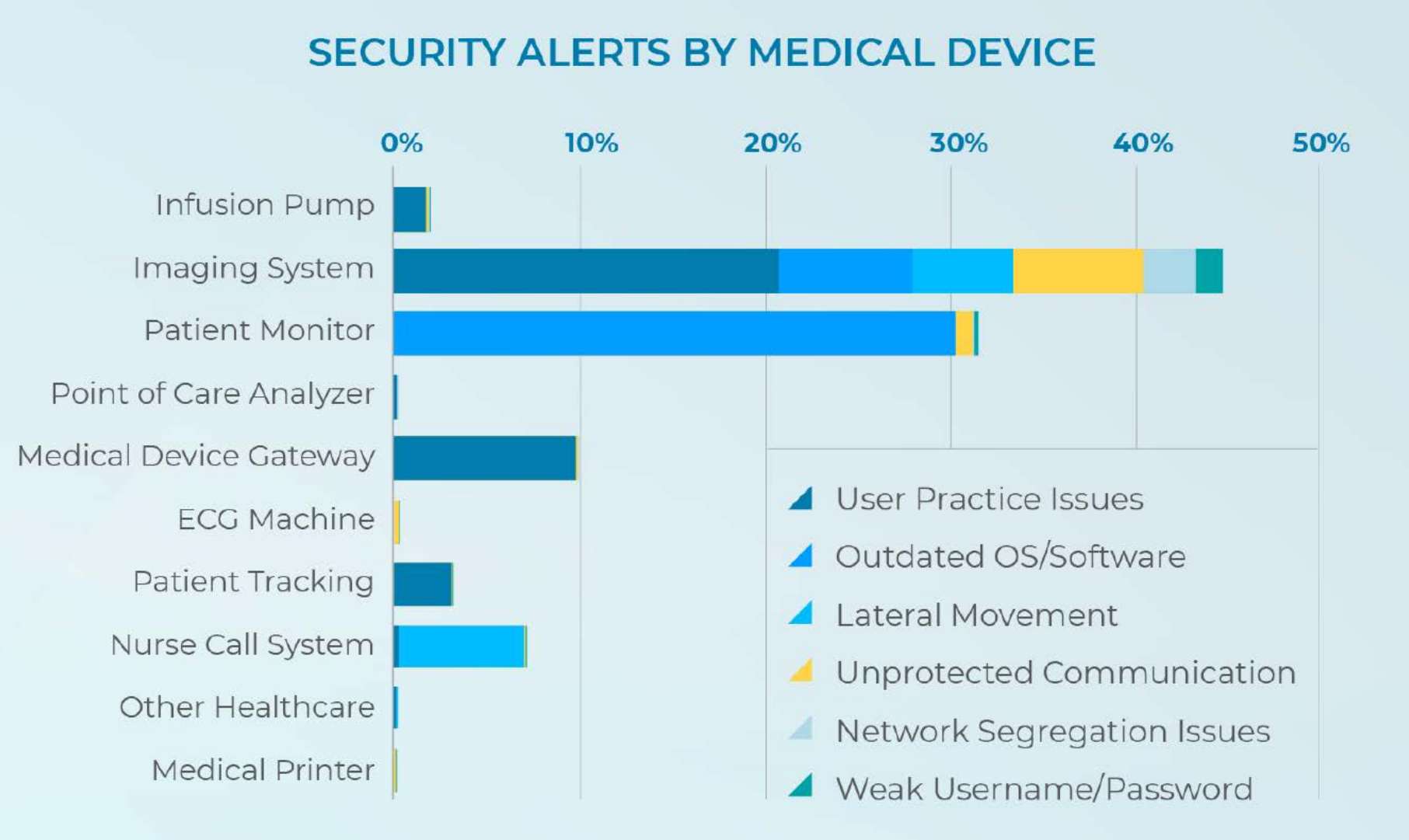
Securing Picture Archiving and Communication System (PACS)

Project Selection



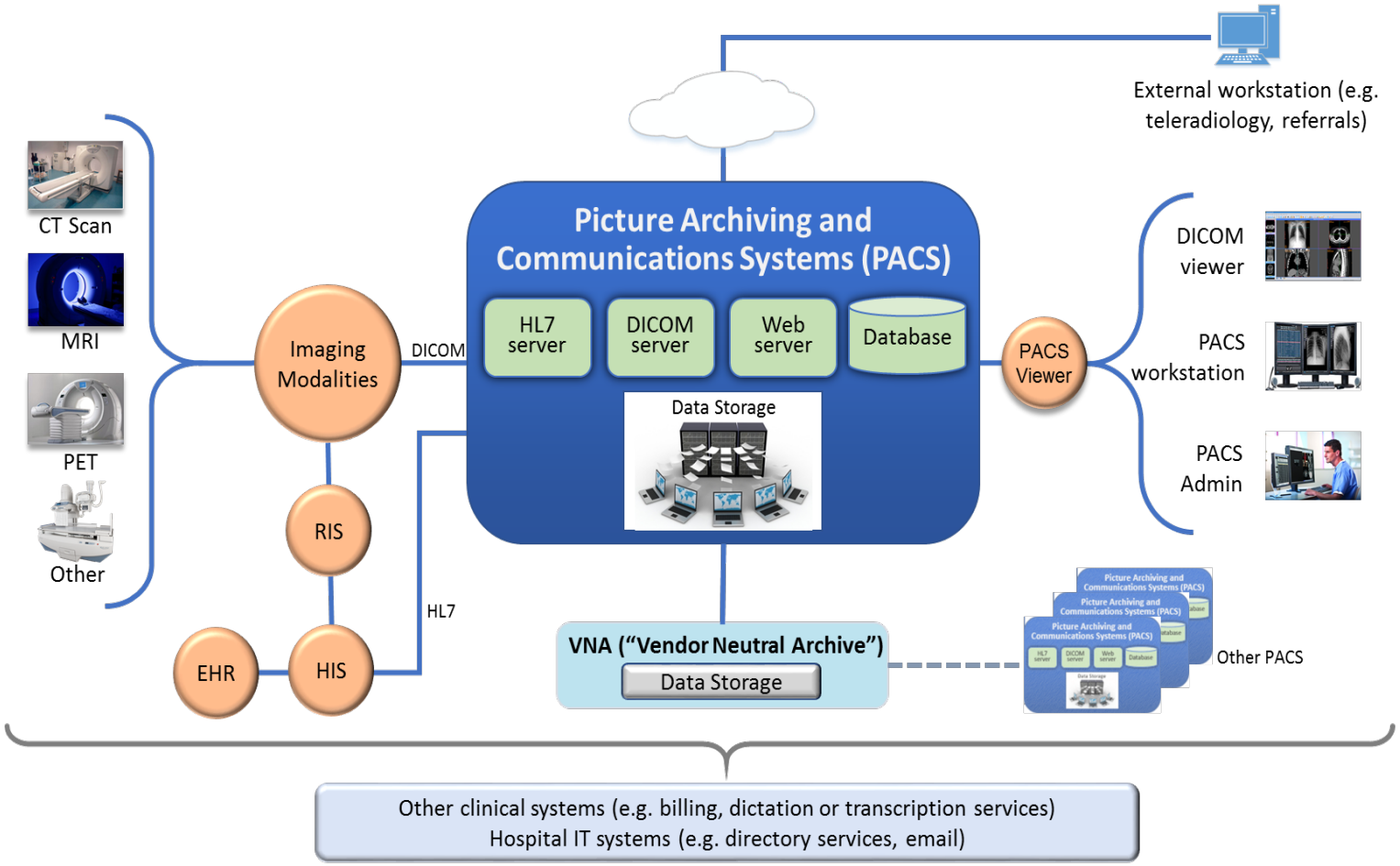
Source: ZingBox, "*Threat Report on IOT Medical Devices*", 1/25/18

Project Selection



Source: ZingBox, "*Threat Report on IOT Medical Devices*", 1/25/18

Picture Archiving and Communication System (PACS)



Final Project Description: https://nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-pacs-project-description-final.pdf

Considering Risks

- Insider Threats
- Data exfiltration
- Misconfiguration
- Service Disruption
- Ransomware


Daily Mail .com

What is WannaCry and who is behind it? Here's all you need to know about the ransomware that crippled the NHS


Healthcare IT News

TOP

Radiology images of 957 patients breached

By Molly Merrill | April 01, 2010 | 10:06 AM

A radiologist contracted by Griffin Hospital, a 160-bed acute care community hospital in St. Derby, Conn., has breached images of 957 patients. The radiologist accessed the reports on the hospital's PACS system, downloaded image files of 339 of these patients, and even contacted some of the patients offering to provide professional services at another area hospital.


HOME / BUSINESS / TECHNOLOGY

The Boston Globe

Beth Israel data breach may affect over 2,000

Virus sent records to unknown location

By Hiawatha Bray

Globe Staff / July 19, 2011


As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FULL BIO

Scenarios

Derived from IHE Radiology Profiles:

- Radiology Practice Workflows
- Accessing Aggregated Images
- Accessing, Monitoring, and Auditing
- Imaging Object Change Management

PACS Schedule

2QFY18: Publish Federal Register Notice (FRN) asking for Collaborators

Products used in the project must be:

- Commercially available
- Addresses one or more of the relevant components
- Addresses one or more of the desired security characteristics

NOTE: NIST/NCCoE does not endorse product or service

PACS Schedule (cont.)

3QFY18: Collaborators sign Cooperative Research and Development Agreement (CRADA) with NIST/NCCoE

3QFY18: Build Team finalized

4QFY18: Build Reference Architecture and write Practice Guide (NIST Special Publication 1800-series)

2QFY19: Publish Draft Practice Guide (NIST Special Publication 1800-series)

Join the NCCoE Healthcare Sector COI: https://nccoe.nist.gov/projects/use-cases/health-it

Questions?

Kevin Stine

kevin.stine@nist.gov

Kevin Littlefield

kevin.littlefield@mitre.org

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov