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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PICTURE ARCHIVING COMMUNICATION SYSTEM

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of securing the Picture Archiving and Communication System (PACS) ecosystem in Healthcare Delivery Organizations (HDOs) by collaborating with industry and the information technology community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Healthcare PACS project, including background and challenge, goals, and potential benefits. If you know of products that might be applicable to the challenge, please contact us at HIT_nccoe@nist.gov.

BACKGROUND

When patients seek medical care, one of the first actions providers take is ordering imaging procedures such as X-Rays or MRIs to help them determine next steps (e.g., determination of health condition, follow-on visits, patient care, etc.). Over the last 10 years, imaging technology has undergone significant changes. For instance, images once processed on film in dark rooms are now digital, and are easily uploaded, stored, and shared. PACS are typically found in image-intensive areas of healthcare such as radiology and often interact with electronic health records, hospital information system, regulatory registries, and multicenter government, academic, and commercial archives. These interactions enable users to easily access images on work or personal devices, giving them the ability to make a diagnosis in a fraction of the time it once required.

CHALLENGE

Common challenges that HDOs face when attempting to secure a PACS are:

- controlling/monitoring and auditing HDO user accounts, including identifying outliers in behavior
- controlling/monitoring and auditing access by users that are external to the HDO, including identifying outliers in behavior that are controlling/monitoring and auditing access and modification to images
- enforcing least privilege and separation-of-duties policies for internal and external users
- ensuring data integrity as imaging moves across the enterprise
- securing and monitoring connections to the HDO ecosystem
- securing and monitoring connections to and from systems external to the HDO
- providing security, data protection, and access management without impacting system performance or user productivity

GOALS

This project will identify the actors interacting with picture archiving and communications systems, define the interactions between the actors and the system, perform a risk assessment, identify applicable mitigating security technologies, and provide an example solution. This work will result in a NIST Cybersecurity Practice Guide, a freely available list of materials and instructions that enable organizations to implement the example solution in their environments.

BENEFITS

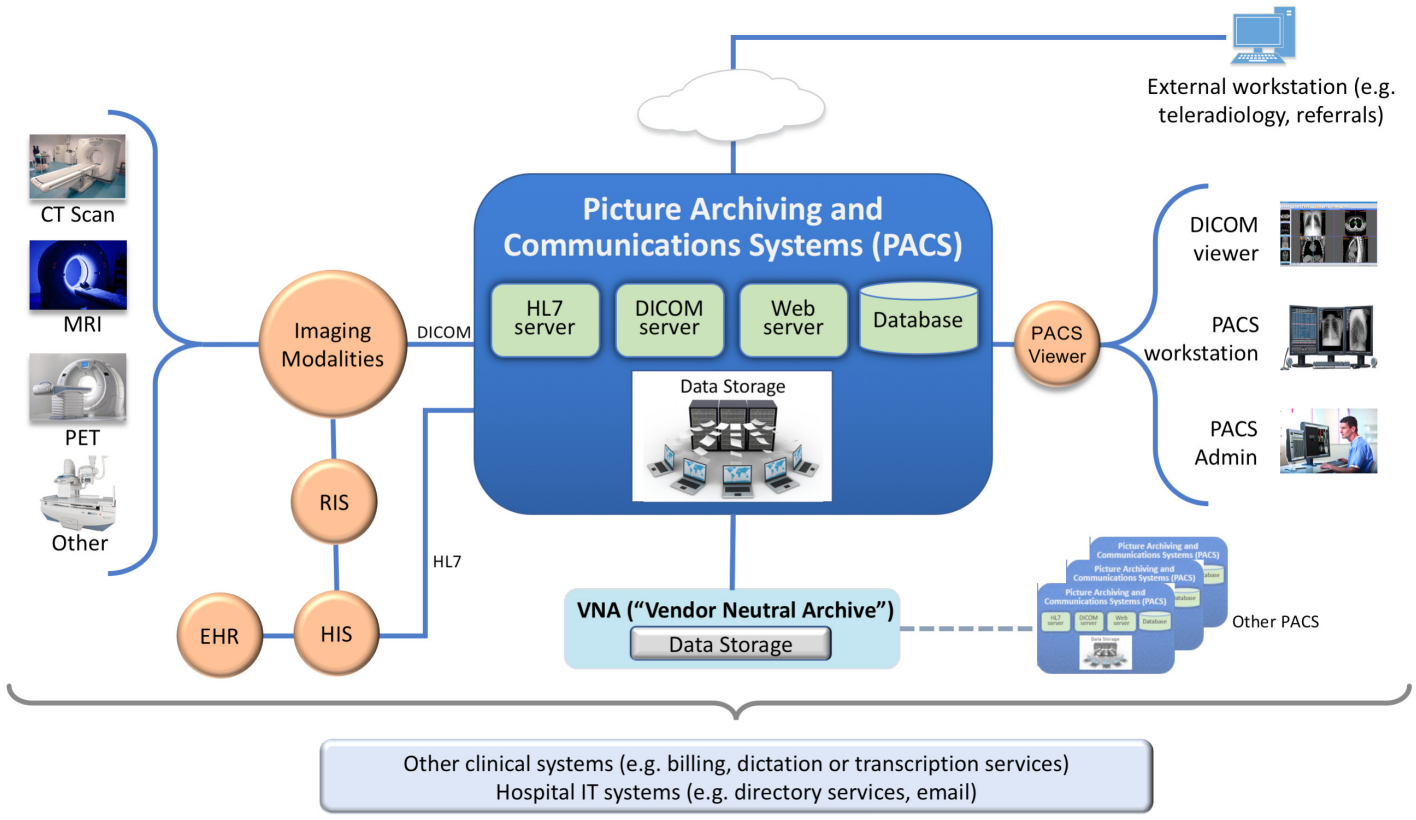
The potential business benefits of enacting stronger security controls to a PACS includes:

- reduces the likelihood of a breach
- reduces risk of significant data losses
- minimizes disruption(s) to a hospital or medical center's systems
- enables timely access to imaging with information less vulnerable to being altered or misdirected
- helps protect patient privacy

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



COMPONENT LIST

The NCCoE has a dedicated lab environment for hosting the development of the example solution, including the following features:

- network with machines using a directory service
- virtualization servers
- network switches
- remote access solution with Wi-Fi and a virtual private network (VPN)

Collaboration partners (participating vendors) will need to provide specialized components and capabilities to realize this solution, including, but not limited to:

- PACS servers, special applications (including web services), and workstations
- Vendor Neutral Archive (VNA)
- data storage
- modality or modality simulator
- Radiology Information System (RIS) or RIS simulator
- notification system
- Electronic Health Record/Electronic Medical Record
- load balancer
- managed service model and remote service connectivity
- certificate management
- authentication mechanism
- session management
- data encryption
- endpoint protection
- encryption
- malware/virus protection
- Host Intrusion Prevention System (HIPS) / Host Intrusion Detection System (HIDS)
- hardware root of trust
- logging, monitoring, security information and event management (SIEM)
- network infrastructure controls
- asset management
- web services

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit: https://nccoe.nist.gov/projects/use-cases/health-it/pacs.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please send an email to HIT_nccoe@nist.gov.

March 2018