NIST SPECIAL PUBLICATION 1800-24

Securing Picture Archiving and Communication System (PACS):
Cybersecurity for the Healthcare Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra
Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Bob Niemeyer
Chris Peloquin
Sue Wang
Ryan Williams
Kangmin Zheng

*Former employee; all work for this publication done while at employer.

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-24

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide

NIST SPECIAL PUBLICATION 1800-24

Securing Picture Archiving and Communication System (PACS):

Cybersecurity for the Healthcare Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Bob Niemeyer
Chris Peloquin
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

FINAL

December 2020

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-24A

Securing Picture Archiving and Communication System (PACS):
Cybersecurity for the Healthcare Sector

Volume A:
Executive Summary

Jennifer Cawthra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Jason Kuruvilla*
Kevin Littlefield
Bob Niemeyer
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

December 2020

FINAL

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-24

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide

Executive Summary

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to emulate a medical imaging environment, performed a risk assessment, and identified controls from the NIST Cybersecurity Framework to secure a medical imaging ecosystem. This project used picture archiving and communication system (PACS) and a vendor neutral archive (VNA) and implemented controls to safeguard medical images from cybersecurity and privacy threats. PACS and a VNA, hereafter referred to as PACS, comprise the systems to centrally manage medical imaging data. This effort resulted in a NIST Special Publication 1800 series Cybersecurity Practice Guide, based on the following considerations relative to PACS:

- PACS allows for the acceptance, transfer, display, storage, and digital processing of medical images. PACS centralizes functions surrounding medical imaging workflows and serves as an authoritative repository of medical image information. Medical imaging is a critical component in rendering patient care. PACS serves as the repository to manage these images and accompanying clinical information within a healthcare delivery organization (HDO).
- PACS fits within a highly complex HDO environment that includes back-office systems, electronic health record systems, and pharmacy and laboratory systems, as well as an array of electronic medical devices. This environment may include cloud storage for medical images. In managing these systems, HDOs work with a diverse group of individuals who interact with the enterprise information technology (IT) infrastructure and may include IT operations staff, internal support teams, and biomedical engineers, as well as vendors and manufacturers.
- Securing PACS presents several challenges. Various departments operating in the HDO have unique medical imaging needs and may operate their own PACS or other medical imaging archiving systems. Further, HDOs may use external medical imaging specialists when reviewing patient medical data. The PACS ecosystem, therefore, may include multiple systems for managing medical imaging data, along with a diverse clinical user community, accessing PACS from different locations. This complexity leads to cybersecurity challenges.
- PACS may have vulnerabilities that, given its central nature, may impact an HDO's ability to render patient care or to preserve patient privacy. These vulnerabilities could impede patients' timely diagnosis and treatment if medical images are altered or misdirected. These vulnerabilities could also expose an HDO to risks of significant data loss, malware and ransomware attacks, and unauthorized access to other parts of an HDO enterprise network.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can securely configure and deploy PACS. This guide presents an example solution that helps HDOs improve medical imaging ecosystem privacy and cybersecurity.

CHALLENGE

PACS, by its nature, is a system that cannot operate in isolation. The overall PACS ecosystem consists of diverse technologies that include medical imaging devices, patient registry systems, and worklist management systems. PACS also relies on systems to manage and maintain medical image archives, which may include cloud storage capabilities. The primary role of PACS is interaction with disparate medical imaging devices, interconnectivity with other clinical systems, and allowing a geographically and organizationally diverse team of healthcare professionals to review medical images to provide quality

and timely patient care. Therefore, the threat landscape is broad, and allows for a large attack surface. The PACS environment may include vulnerabilities. Unauthorized individuals may leverage vulnerabilities and compromise or corrupt stored information. Also, unauthorized individuals may use components found in the PACS ecosystem as pivot points to further compromise components in an integrated healthcare information system.

SOLUTION

This practice guide demonstrates how an organization may implement a solution to mitigate identified cybersecurity and privacy risks. The reference architecture features technical and process controls to implement:

- a defense-in-depth solution, including network zoning that allows more granular control of network traffic flows and limits communications capabilities to the minimum necessary to support business function
- access control mechanisms that include multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components
- a holistic risk management approach that includes medical device asset management, augmenting enterprise security controls, and leveraging behavioral analytic tools for near real-time threat and vulnerability management in conjunction with managed security solution providers

The NCCoE sought existing technologies that provided the following capabilities:

- role-based access control
- microsegmentation
- behavioral analytics
- data security
- cloud storage

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide, *Securing Picture Archiving and Communication Systems*, can help your organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO environment by authorized system users to address the "insider threat" as well as limit unauthorized actors once they gain network access

- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential advanced persistent threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information) at rest, in transit, and in cloud environments; enhancing patient privacy by limiting malicious actors' ability to exfiltrate or expose that data
- consider and address risks that may be identified as HDOs examine cloud storage solutions as part of managing their medical imaging infrastructure

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hit_nccoe@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The NCCoE, a part of NIST, is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-24B

Securing Picture Archiving and Communication System (PACS):
Cybersecurity for the Healthcare Sector

Volume B:
Approach, Architecture, and Security Characteristics

Jennifer Cawthra
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Bob Niemeyer
Chris Peloquin
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

December 2020

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-24

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name of company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-24B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24B, 102 pages, (December 2020), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Medical imaging plays an important role in diagnosing and treating patients. The system that manages medical images is known as the picture archiving communication system (PACS) and is nearly ubiquitous in healthcare environments. PACS is defined by the Food and Drug Administration (FDA) as a Class II device that "provides one or more capabilities relating to the acceptance, transfer, display, storage, and digital processing of medical images." PACS centralizes functions surrounding medical imaging workflows and serves as an authoritative repository of medical image information.

PACS fits within a highly complex healthcare delivery organization (HDO) environment that involves interfacing with a range of interconnected systems. PACS may connect with clinical information systems and medical devices and engage with HDO-internal and affiliated health professionals. Complexity may introduce or expose opportunities that allow malicious actors to compromise the confidentiality, integrity, and availability of a PACS ecosystem.

The NCCoE at NIST analyzed risk factors regarding a PACS ecosystem by using a risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework and other relevant standards to identify measures to safeguard the ecosystem. The NCCoE developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem. This practice guide helps HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk and protect patient privacy while maintaining the performance and usability of PACS.

KEYWORDS

access control; auditing; authentication; authorization; behavioral analytics; cloud storage; DICOM; EHR; electronic health records; encryption; microsegmentation; multifactor authentication; PACS; PAM; picture archiving and communication system; privileged account management; vendor neutral archive; VNA

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Matthew Hyatt	Cisco
Kevin McFadden	Cisco
Cletis McLean	Cisco
Peter Romness	Cisco
Deidre Cruit	Clearwater Compliance
Mike Nelson	DigiCert
Taylor Williams	DigiCert

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
Joseph Davis	Microsoft
Janet Jones	Microsoft
Dan Menicucci	Microsoft
Mehwish Akram	The MITRE Corporation
Steve Edson	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Harry Perper	The MITRE Corporation
David Alfonso	Philips Healthcare
Jonathan Bagnall	Philips Healthcare
Julian Castro	Philips Healthcare
Sukanta Das	Philips Healthcare
Jason Dupuis	Philips Healthcare
Michael McNeil	Philips Healthcare

Name	Organization
Dwayne Thaele	Philips Healthcare
Steve Kruse	Symantec
Derek Peters	Symantec
Axel Wirth	Symantec
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Robert Armstrong	Tempered Networks
Nicholas Ringborg	Tempered Networks
Randy Esser	Tripwire
Onyeka Jones	Tripwire
Jim Wachhaus	Tripwire
Sandra Osafo	University of Maryland University College
Henrik Holm	Virta Labs
Michael Holt	Virta Labs
Ben Ransford	Virta Labs
Jun Du	Zingbox
Damon Mosk-Aoyama	Zingbox
David Xiao	Zingbox

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Cisco Firepower Version 6.3.0 Cisco Stealthwatch Version 7.0.0
Clearwater Compliance	Clearwater Information Risk Management Analysis
DigiCert	DigiCert PKI Platform
Forescout	Forescout CounterACT 8
Hyland	Hyland Acuo Vendor Neutral Archive Version 6.0.4 Hyland NilRead Enterprise Version 4.3.31.98805 Hyland PACSgear Version 4.1.0.64
Microsoft	Azure Active Directory (AD) Azure Key Vault Version Azure Monitor Azure Storage Azure Security Center Version Standard Azure Private Link
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
Symantec, a division of Broadcom	Symantec Endpoint Detection and Response (EDR) Version 4.1.0 Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7 Symantec Endpoint Protection (SEP 14) Version 14.2 Symantec Validation and ID Protection Version 9.8.4 Windows

Technology Partner/Collaborator	Build Involvement
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
Tripwire	Tripwire Enterprise Version 8.7
Virta Labs	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

Contents

List of Figures

List of Tables

1 Summary

Medical imaging is a critical component in rendering patient care. The system that provides the acceptance, transfer, display, storage, and digital processing of medical images is known as a picture archiving and communication system (PACS) [1] and is nearly ubiquitous in healthcare environments. The PACS environment serves as the repository to manage these images and accompanying clinical information within the healthcare delivery organization (HDO). Vendor neutral archive systems (VNAs) perform archive management functions similar to PACS, and hereafter, this practice guide includes VNAs when it refers to PACS. PACS fits within a highly complex HDO environment and may interface with a range of enterprise information technology (IT) systems and healthcare professionals internal and external to the HDO. This complexity leads to cybersecurity challenges.

To develop practical cybersecurity guidance for securing PACS, we must consider the ecosystem surrounding PACS, which includes interconnected medical imaging equipment generally described as modalities. The ecosystem also includes modalities; connected clinical systems such as radiology information systems (RIS), health information systems (HIS), or the electronic health record (EHR); cloud storage capabilities; viewer and administration workstations; VNAs; and the PACS itself.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory that emulates a medical imaging environment, performed a risk assessment, and developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem. Any organization that deploys PACS and medical imaging systems can use the example implementation, which represents one of many possible solutions and architectures, but those organizations should perform their own risk assessment and implement controls based on their risk posture.

For ease of use, the following paragraphs provide a short description of each section of this volume.

Section 1, Summary, presents the challenge addressed by the NCCoE project, with an in-depth look at our approach, the architecture, and the security characteristics we used; the solution demonstrated to address the challenge; benefits of the solution; and the technology partners who participated in building, demonstrating, and documenting the solution. The Summary also explains how to provide feedback on this guide.

Section 2, How to Use This Guide, explains how business decision makers, program managers, IT professionals (e.g., systems administrators), and biomedical engineers might use each volume of the guide.

Section 3, Approach, offers a detailed treatment of the scope of the project, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

Section 4, Architecture, specifies the components within the PACS ecosystem from business, security, and infrastructure perspectives and details how data and processes flow throughout the ecosystem. This section also describes the security capabilities and controls referenced in the NIST Cybersecurity Framework through tools provided by the project collaborators.

Section 5, Security Characteristic Analysis, provides details about the tools and techniques used to perform risk assessments pertaining to PACS.

Section 6, Functional Evaluation, summarizes the test sequences employed to demonstrate security platform services, the NIST Cybersecurity Framework Functions to which each test sequence is relevant, and the NIST Special Publication (SP) 800-53 Revision 4 controls demonstrated in the example implementation.

Section 7, Future Build Considerations, is a brief treatment of other applications that NIST might explore in the future to further protect a PACS ecosystem.

The appendixes provide acronym translations, references, a mapping of the PACS project to the NIST Cybersecurity Framework, and a list of additional informative security references cited in the framework. Acronyms used in figures and tables are in the List of Acronyms appendix.

1.1 Challenge

The challenge with PACS is securing disparate, interconnected systems. A medical imaging infrastructure offers a broad attack surface with equipment that may have varying vulnerabilities, configurations, and control implementations. Devices deployed in the ecosystem likely come from different vendors and suppliers, and how one may implement defensive measures can vary based on the nature of the devices and how they function vis-à-vis patients and other clinical systems. The ecosystem may also include legacy devices that are potentially more vulnerable to cyber risks. The care provider team (clinicians and other healthcare professionals) may reside in different departments and may have components hosted and used across a wide geography. HDOs may leverage cloud storage environments to store and maintain medical images. Some actors may be external to the HDO, interacting with sensitive information across the internet.

As threats to the operational environment increase, PACS and other healthcare systems may become increasingly vulnerable to:

- system disruption, leading to
  - inability to render timely diagnosis and treatment
  - inability to access the system for standard use, including inability to schedule procedures
- compromise of image data, leading to incorrect diagnosis and treatment

- compromise of components, allowing malicious actors to use the components as pivot points to attack other parts of the HDO infrastructure
- privacy concerns that may lead to
  - fraudulent or improper use of data
  - patient identity theft

1.2 Solution

This NIST Cybersecurity Practice Guide, *Securing Picture Archiving and Communication System (PACS)*, shows how biomedical engineers, networking engineers, security engineers, and IT professionals can help securely configure and deploy PACS within HDOs by using commercially available, open-source tools and technologies that are consistent with cybersecurity standards.

This practice guide leveraged the NIST Cybersecurity Framework in selecting privacy and cybersecurity controls. Controls and solutions may be procured, obtained as part of an open-source solution, or internally developed. While the NCCoE obtained commercially available products for this practice guide, these do not represent the only methods available to HDOs in meeting control objectives.

The reference architecture features technical and process controls to implement the following solutions:

- a defense-in-depth solution, including network zoning that allows more granular control of network traffic flows and limits communications capabilities to the minimum necessary to support business function
- access control mechanisms that include multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components
- a holistic risk management approach that includes medical device asset management augmenting enterprise security controls. It should also leverage behavioral analytic tools for near real-time threat and vulnerability management in conjunction with managed security solution providers
- cloud storage for medical images, which makes images scalable and available for HDOs

1.3 Benefits

The NCCoE's practice guide to securing PACS in HDOs can help your organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO enterprise network to address the potential risk of an insider threat or malicious actors who gain network access

- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information [PHI]) at rest, in transit, and in cloud environments; enhance patient privacy by limiting malicious actors' ability to exfiltrate or expose that data
- consider and address risks of potential cloud solutions to manage an HDO's medical imaging infrastructure

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to help secure a medical imaging ecosystem. This practice guide builds upon the network zoning concept described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*. As part of the implementation, the project used microsegmentation, role-based access controls, and behavioral analytics in the lab's security controls. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-24A: *Executive Summary*
- NIST SP 1800-24B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-24C: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-24A, which describes the following topics:

- challenges that enterprises face in securing PACS
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-24B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- Section 3.5, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary,* NIST SP 1800-24A, with your leadership team members to help them understand the importance of adopting standards-based, commercially available technologies that can help secure a PACS ecosystem.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-24C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the NCCoE's risk assessment and deployment of a defense-in-depth strategy. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

An HDO enterprise network environment is complex, with IT infrastructure to handle a range of functions, including back office billing, supply chain and inventory management, EHRs, and a vast array of connected medical devices. PACS serves an important function within this already complex environment through its role in aggregating and centralizing the medical imaging ecosystem while interfacing with other clinical systems. Specialists involved in the workflow may reside in different departments, be in different parts of an HDO campus, and be external to the HDO, accessing systems and images from the internet. This practice guide seeks to help the healthcare community evaluate the security environment surrounding PACS and medical imaging in a clinical setting.

Throughout the Securing PACS project, we collaborated with our NCCoE Healthcare Community of Interest and technology and cybersecurity vendors to identify standard medical imaging workflows and actors, define interactions between actors and systems, and review risk factors. Based on this analysis, the NCCoE developed an architecture and reference design, identified applicable mitigating security technologies, and designed an example implementation to help better secure a PACS ecosystem. This volume provides the approach used to develop the NCCoE reference solution. Elements include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping.

To develop the reference solution, we reviewed known vulnerabilities in PACS, the Digital Imaging and Communications in Medicine (DICOM) protocol [2], [3], and medical imaging process flow, leveraging

use cases described by Integrating the Healthcare Enterprise (IHE) [4]. We examined how to design the architecture and component integration to increase the security of the device.

The practice guide used the systems security engineering (SSE) framework discussed in NIST SP 800-160 Volume 1 [5] to introduce a disciplined, structured, and standards-based set of SSE activities and tasks to the project. This SSE framework provides the starting point and the forcing function to introduce engineering-driven actions that lead to more defensible and resilient systems. The SSE framework starts with and builds upon standards for systems and software engineering, then introduces SSE techniques, methods, and practices into these standard system engineering processes.

Additionally, this project reviewed NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [6], as well as NIST SP 800-181 Rev.1, *Workforce Framework for Cybersecurity (NICE Framework)* [7], for further guidance. Organizations may refer to these documents in expanding their safeguarding environment as appropriate. These documents serve as background for this project, with primary emphasis on the NIST Cybersecurity Framework [8] and the NIST Risk Management Framework [9].

3.1 Audience

The NCCoE provides this guide for professionals implementing security solutions within an HDO. It may also be of interest to anyone responsible for securing nonstandard computing devices (i.e., the Internet of Things [IoT]). More specifically, the NCCoE designed Volume B of this practice guide (NIST SP 1800-24B) to appeal to a wide range of job functions, including IT operations, storage support engineers, network engineers, PACS support biomedical engineers, cybersecurity engineers, healthcare technology management (HTM) professionals, and support staff who are responsible for medical imaging devices, viewing or administrative workstations, PACS, or VNAs. For cybersecurity or technology decision makers within HDOs, this volume provides a view into how they can make the medical device environment more secure, to help improve their enterprise's security posture and reduce enterprise risk. Additionally, this volume offers guidance to technical staff on building a more secure medical device network and instituting compensating controls.

3.2 Scope

The NCCoE project focused on securing the environment of a PACS ecosystem but not on reengineering medical devices or altering medical imaging processes themselves. This project led to a standards-based practice guide that applies to the wider healthcare ecosystem. This practice guide describes how the project secured PACS in a laboratory environment at the NCCoE that replicated parts of a typical HDO environment. The project considered PACS users internal to the HDO as well as external users and partners needing access to certain components of the HDO environment.

3.3 Assumptions

In building this healthcare practice guide, the NCCoE began the project with the following fundamental assumptions:

- Medical devices will include flaws or weaknesses that may be leveraged as vulnerabilities.
- Patches or fixes for these vulnerabilities may not be available or deployable in a timely fashion.
- Other components within an HDO's network may include flaws and vulnerabilities.
- Security controls that one may deploy may themselves include flaws or weaknesses that could be used to compromise the HDO network.

This practice guide identifies controls that may be appropriate for mitigating risks associated with the medical imaging ecosystem made up of PACS and VNA. The actual build and example implementation of this architecture occurred in a lab environment at the NCCoE. Although the lab is based on a clinical environment, it does not mirror the complexity of an actual hospital network. It is assumed that any actual clinical environment would represent additional complexity. As a result, in addition to the assumptions noted above, we also assume implementation of pervasive controls, discussed in more detail in Appendix C.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [10], states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [11]—material that is available to the public. The Risk Management Framework (RMF) [9] guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

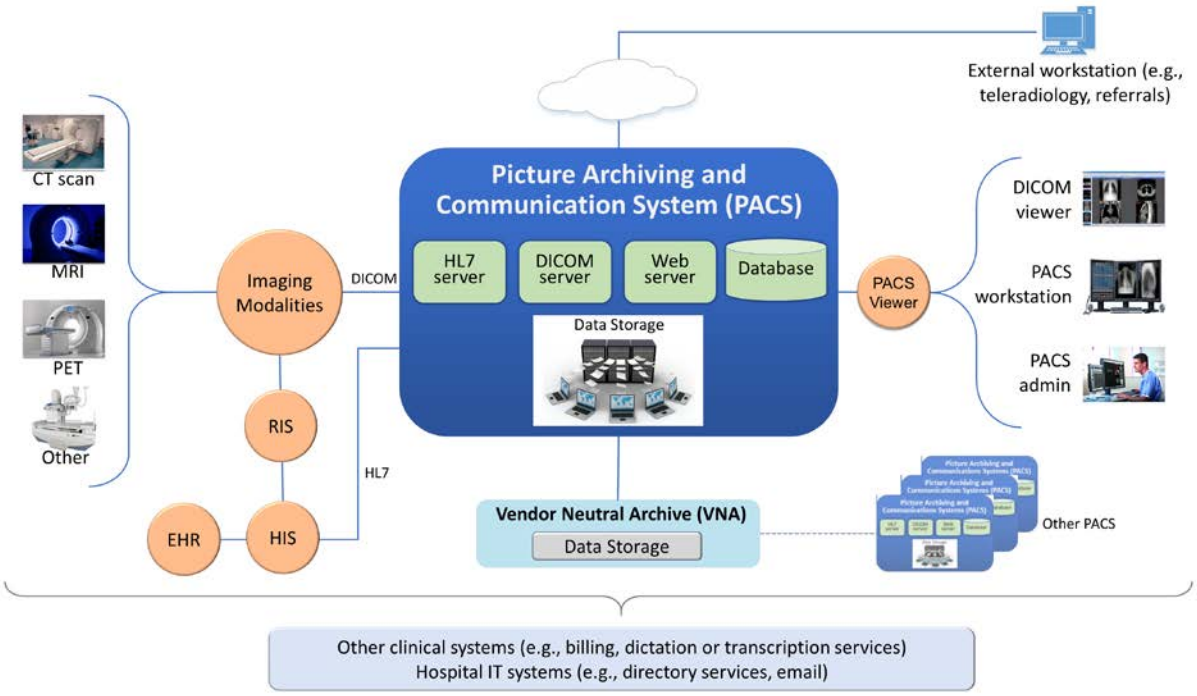
In conducting the risk assessment, this document considers threats and risks grouped under Confidentiality, Integrity, and Availability, commonly referred to as the CIA triad [12].

3.4.1 Establishing the Risk Context

As we examine risk, we begin by considering the risk context. The ecosystem itself is complex and presumes different teams of people, varying processes, and different technologies involved in acquisition, interpretation, and maintenance of medical imaging information. This section presents the risk context of the Securing PACS Project, which is established around five scenarios that represent typical processes found in a medical imaging ecosystem [13]. The risk context, which in this practice guide is within the medical imaging ecosystem logical boundary, defines where to perform a risk assessment. Risk context of the PACS environment encompasses the physical and logical components of the medical imaging ecosystem that interconnect with PACS as well as the various stakeholders within the ecosystem. For the NCCoE PACS lab environment, risk context contains the components listed below and the system actors of the PACS, which include both human and system actors, as described in Section 3.4.2.

Figure 3-1 depicts the notional high-level architecture that bounds the PACS and medical imaging ecosystem [13]. This depiction provides a starting point in understanding the components addressed in this project. However, this project took a holistic approach in framing the risk context, beyond some of the technology components. This project leveraged concepts described in NIST SP 800-160 [5] in defining context for a PACS ecosystem, understanding risk based on context, and selecting appropriate controls when designing the control environment needed to mitigate that contextual risk. NIST SP 800-160, *Systems Security Engineering* [5], identifies concepts of examining system life cycle and components, performing holistic analysis on both technical and nontechnical processes, to deliver "trustworthy" systems. Trustworthiness describes a solution whose objective is to provide "adequate security" related to stakeholders' concerns. In order to achieve systems security engineering "trustworthiness" goals, practitioners should consider system life-cycle processes and frame the risk context based on a process and entity relationship analysis [5].

Figure 3-1 Notional High-Level Architecture



The system for this project is broadly identified as the PACS, though practically, it incorporates a set of processes and other systems that make up a medical imaging ecosystem [13]. For purposes of this project, and in accordance with NIST SP 800-160 [5], we consider the individual components as "systems of interest," noted below:

- workstations used to interact with the medical imaging ecosystem
  - viewer workstations residing within the HDO perimeter
  - viewer workstations residing external to the HDO perimeter, used by remote care specialists
  - workstations used by clinical staff to access peripheral systems, such as order entry systems, RIS, HIS, or EHR
- modalities, or medical imaging devices that acquire medical images and forward those to the PACS, based on orders typically received from the EHR or HIS and following workflows typically defined by the RIS
- clinical systems that interface with modalities and the PACS environment, supporting medical imaging processes such as scheduling, annotations, or reporting

- PACS will support interfaces, depicted in Figure 3-1, as "servers." These interfaces include the Health Level 7 (HL7) interface that allow clinical systems to interact with the PACS in sharing PHI; the DICOM interface, which represents a communications and medical imaging standard that represents a standard method by which medical imaging modalities interoperate with PACS; and the web server interface, which represents the PACS' ability to allow clinical interaction with the PACS to retrieve medical images using hypertext transfer protocol (http) via a standard web browser.
- a relational database server to manage metadata about the medical images or PACS administration data
- PACS and vendor neutral archive (VNA) application servers

In addition to the technology components described above and in the PACS Project Description, we considered other elements, such as stakeholders (system actors) as well as specific business process flows in which those stakeholders may participate. The processes align with profiles established by Integrating the Health Enterprise (IHE) [4], which this project leveraged to determine process and data flows. The four selected profiles translate to the scenarios described below. Based on the PACS Project Description document, the scenarios of note are Sample Radiology Practice Workflows; Access to Aggregations and Collections of Different Types of Images; Accessing, Auditing, and Monitoring; Image Object Change Management; and Remote Access [13].

This practice guide does not examine pervasive risks that an HDO may face but rather focuses on those risks specific to the medical imaging ecosystem. While this guide suggests specific requirements for safely and securely hosting PACS, the intent of the guide is not to serve as an omnibus guide for all facets potentially required to operate a secure HDO infrastructure. This guide addresses measures that would enhance the security posture for the overall PACS and medical imaging ecosystem, but there may be elements that HDOs should address beyond the recommendations offered in safeguarding a PACS and the overall medical imaging ecosystem.

3.4.2 System Actors

This project considered several roles that interact with the PACS and medical imaging system ecosystem. This project looked at both authorized human and system actors. Human actor roles consist of:

- medical imaging technologists
- clinicians
- clinical systems IT administrators
- HTM professionals
- IT staff

System actors that interact with the PACS and VNA consist of:

- modalities
- RIS and HIS
- EHRs

The system actor list excludes patients. The actions focused on medical images, which include creation of the image, annotation, storage of the image and annotations, interpretation, and changes to those images. The project limited radiology information systems and EHR systems actions to order entry/scheduling procedures and to pointing to images for reading/viewing. The scenarios below note process flows which describe use case profiles defined by IHE, a body that this project identified as authoritative in defining standard imaging workflow processes [4].

3.4.3 Use Case Scenarios

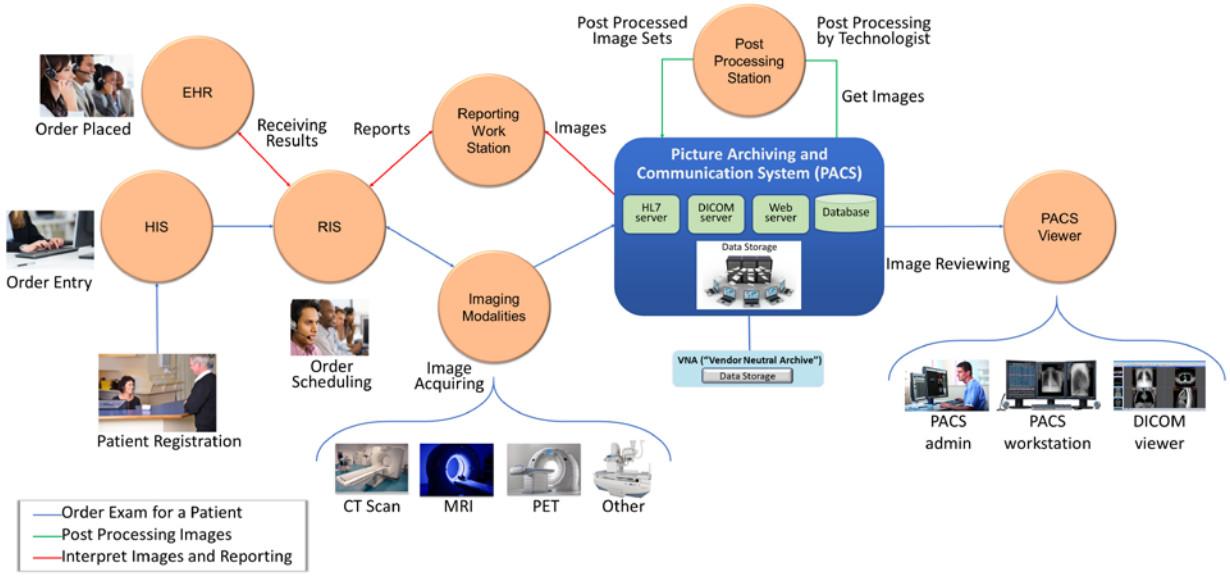
This project assessed risk for the five scenarios [13] described below. Considering threats, vulnerabilities, likelihoods, and impacts on medical imaging operations under these scenarios contributed to the risks documented in Section 3.4.6.

These scenarios frame the processes wherein we considered introduction of threats. In addition to the scenario, this document investigates those vulnerabilities, threats, and risks that may be evident based on a holistic view of the architecture, as described in Section 3.4.4, Section 3.4.5, and Section 3.4.6. Within that viewpoint, the scenarios excluded several threats that are relevant for consideration. While this document investigates addressing modality interfaces, it does not examine specific modalities or the risks potentially associated with them. Modality devices themselves are medical devices that may include vulnerabilities or opportunity for systems or data compromise, loss of data integrity, or disruption of service, and HDOs should perform independent risk assessments in addressing those risks.

3.4.3.1 Sample Radiology Practice Workflows

Scenario One, shown in Figure 3-2, starts with registration of a patient who requires an imaging procedure be performed [13]. For the purposes of this project, the assumption is that the HDO registers the patient into the EHR, determines the patient has appropriate identifiers to be admitted, and the patient is able to receive procedures. The scenario follows the process flow that begins at scheduling the procedure, acquiring the image, and allowing the care team to analyze and diagnose. The assumption is that all modality devices and clinical staff are on-premise, within the boundaries of the HDO. Systems in this sample radiology practice workflow convey patient information using the HL7 [14] protocol (e.g., patient registration and order entry messages). Medical imaging devices would interact with the PACS/VNA by using DICOM [2], [3].

Figure 3-2 Scenario One: Sample Radiology Practice Workflows



The scenario's processes are as follows:

- **Patient Registration:** The HDO enters a new patient's information into an HIS. An HIS may also be referred to as a clinical information system. The function of this process flow is to establish a patient identity within a hospital where one may not previously exist and then administer the patient as appropriate.
- **Order Entry:** Once the HDO establishes a patient identity, a clinician can order a medical imaging procedure for the patient by using some form of computerized physician order entry system.
- **Order Scheduling:** Following a submitted order, clinicians may schedule a medical imaging procedure involving an appropriate medical imaging modality using a RIS.
- **Image Acquisition:** After a clinician creates an order and scheduling has been performed, a clinician performs the imaging procedure using the appropriate modality. Acquisition results in creation of a medical image.
- **Image Post-Processing:** When the modality creates the medical image, imaging technologists will examine the image and may record initial annotations. The image and annotations are then pushed to the PACS.
- **Image Analysis and Reporting:** An imaging clinician may use a viewer workstation to examine the image, analyze, interpret, and diagnose, with subsequent notes pushed to the PACS for reporting.

Stakeholders: medical imaging technologists, clinicians (medical imaging specialists), and medical imaging devices (modalities)

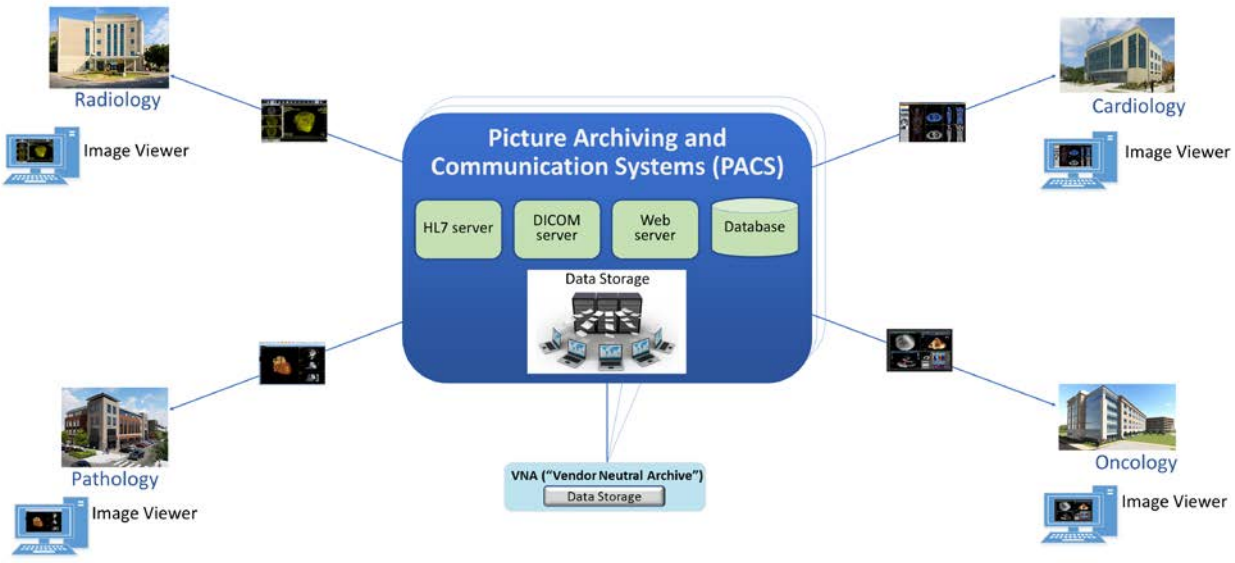
Systems of Interest: order entry, RIS, medical imaging devices, viewer workstations, PACS

Protocols Used: DICOM, web (e.g., hypertext transfer protocol secure [https]), HL7, Host Identity Protocol (HIP)

3.4.3.2 Image Data Access Across the Enterprise

Scenario Two, as shown in Figure 3-3, examines multiple departments that use disparate imaging devices for acquisition and may involve multiple PACS [13]. The assumption is that different departments have separate clinical staff and different medical imaging goals and may use different means to centralize their medical images. This scenario simulates a hospital, in that radiology is not the only department that uses medical imaging, nor does the radiology department mandate use of its PACS to centralize medical images across a hospital. Aggregation and centralized management remain the goal, but the practice guide describes other components in the ecosystem that enable broader clinical functionality. While PACS implements central medical image storage, access to images is not permitted for all clinical staff.

Figure 3-3 Scenario Two: Image Data Access Across the Enterprise



In demonstrating that different groups and technologies are involved, this project shows variables as "_a" or "_b." This allows us to show the separation between two components that may be similar in function but are separate, e.g., "component_a" versus "component_b."

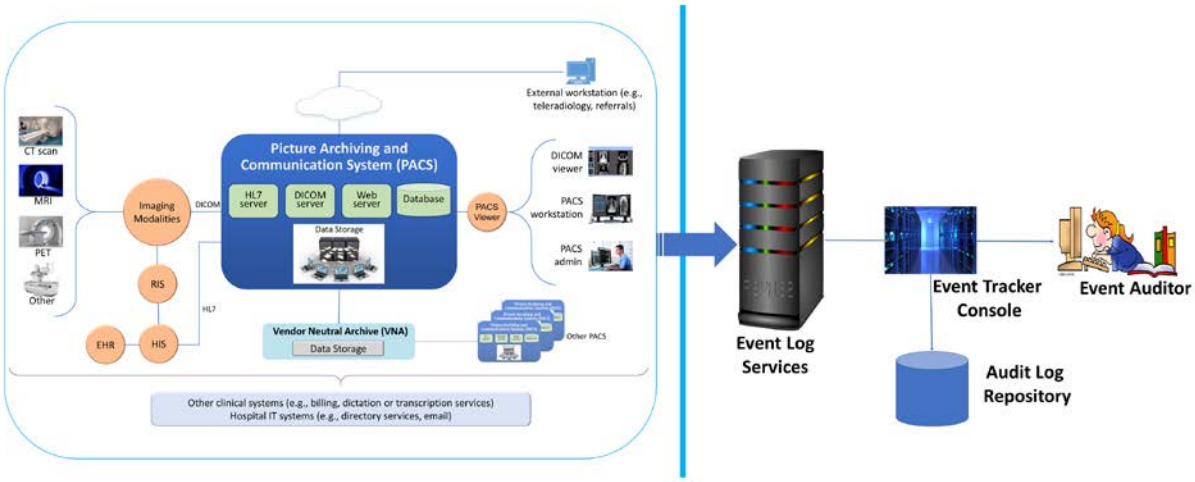
Stakeholders: medical imaging staff_a, medical imaging staff_b, healthcare technology management professionals, PACS_a, PACS_b, VNA

Systems of Interest: image viewer_a, image viewer_b, PACS_a, PACS_b, VNA

3.4.3.3 Accessing, Monitoring, and Auditing

Scenario Three, as shown in Figure 3-4, examines the infrastructure required for access control, which includes identity management and authentication for actors who interact with the PACS and VNA environments, as well as logging, auditing, and monitoring actions with the stored information [13]. The scenario considers those actions where individuals or devices retrieve and view information (Read actions) and introduce new information (Write actions), as well as when individuals or devices modify stored information (Change actions).

Figure 3-4 Scenario Three: Accessing, Monitoring, and Auditing



This project established identities for users (humans who interact with the system), as well as for devices and systems. This scenario assumed that individuals have been appropriately identity-proofed and are provisioned accounts with which they may access and use viewer applications. Given that this project provisioned identities and accounts for both human and machine actors, all interactions require authentication. Authentication may involve exchange of passwords, passcodes, biometrics, or cryptographic keys to validate the actor. A log file recorded all transactions, including authentication attempts.

This scenario examines clinical use system interaction and does not address privileged user access. Controls to manage privileged access are discussed in Section 4.1.5.1.1, Privileged Access Management.

Stakeholders: medical imaging staff, medical devices, PACS, VNA

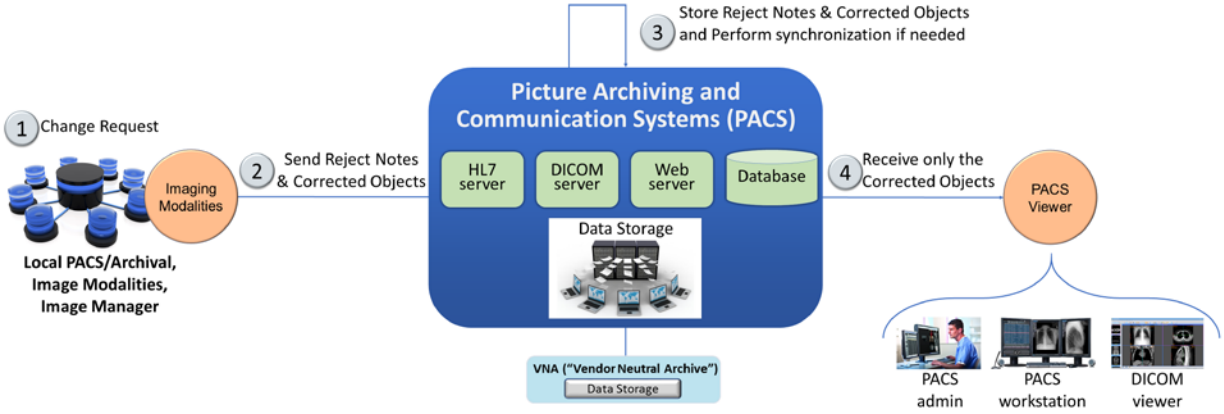
Systems of Interest: directory servers, user account systems, digital certificate servers

Protocols: public key infrastructure (PKI) (associated protocols such as Certificate Management Protocol, http, https), domain name system (DNS), Active Directory

3.4.3.4 Imaging Object Change Management

Scenario 4, as shown in Figure 3-5 , supports the changes that include (1) object rejection due to quality or patient safety reasons, (2) correction of incorrect modality worklist entry selection, and (3) expiration of objects due to data retention requirements [13]. This diagram depicts the change request process. The scenario considers those actions when an authorized healthcare professional, upon review of the image, determines that errors or qualitative defects found in an image may lead to an inappropriate conclusion.

Figure 3-5 Scenario Four: Imaging Object Change Management



Stakeholders: medical imaging clinicians

Systems of Interest: PACS, VNA

Protocols: HL7, http, https

3.4.3.5 Remote Access

Scenario 5, depicted in Figure 3-6, supports external parties who may need access to the PACS ecosystem. The scenario provides a pathway for IT vendors to provide remote systems support as well as for third-party clinical participants to interact with the PACS. IT vendors may consist of clinical systems support staff who may need to help maintain the PACS or VNA system. Third-party clinical participants may consist of medical imaging specialists or teleradiology specialists who may need to review medical images acquired at the HDO.