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