PROJECT DESCRIPTION

SECURING PICTURE ARCHIVING AND COMMUNICATION SYSTEM (PACS)

Cybersecurity for the Healthcare Sector

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

Kevin Littlefield
Robert Niemeyer
Sue Wang
Kangmin Zheng
The MITRE Corporation

January 2018
hit_nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity challenges with practical, standards-based solutions using readily available commercial and open-source technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a cybersecurity challenge that is relevant across the healthcare sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the healthcare sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by Healthcare Delivery Organizations (HDOs).

ABSTRACT

Picture Archiving and Communication System (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. Its hardware components may include workstations, digitizers, communications devices, computers, video monitors, magnetic, optical disk, or other digital data storage devices, and hardcopy devices. The software components may provide functions for performing operations related to image manipulation, enhancement, compression or quantification." [1]

PACS is nearly ubiquitous in hospitals, prompting the Healthcare Sector Community of Interest to identify securing PACS as a critical need. PACS ties into doctor-patient workflow management, where results based on image interpretation determine the patient's next steps (e.g., determination of health condition, follow-on visits, patient care, other actions). PACS is typically found in image-intensive areas of healthcare (e.g., Radiology, Cardiology, Orthopedics, Pathology, Ophthalmology). Although the PACS fundamentals across clinical disciplines are similar, there are several significant differences due to varying clinical requirements. Therefore, PACS requires controls that provide significant integrity, availability, and confidentiality assurances.

PACS allows for remote image review by users from within the HDO infrastructure and external to the HDO infrastructure. PACS typically interacts with electronic health records (EHRs); Hospital Information System (HIS); Radiology or Cardiology Information System (RIS/CIS); diagnostic reporting; vendor neutral archive; regulatory registries; and multicenter government, academic, and commercial archives. Users access PACS by using HDO-supplied and configured devices, and personal devices. The amorphous aspect of PACS exposes a threat vector that could act as a point where an attack may be performed or may serve as a pivot point into an integrated healthcare information system.

The goal of this project is to provide a practical solution for securing the PACS ecosystem. The project team will perform a risk assessment on a representative PACS ecosystem in the laboratory environment, apply the NIST cybersecurity framework and guidance based on medical device standards, and collaborate with industry and public partners. The result will be a freely available NIST Cybersecurity Practice Guide that includes a reference design and a detailed description of the practical steps needed to implement the solution based on standards and best practices.

KEYWORDS

Access control, auditing, authentication, authorization, DICOM, encryption, life cycle management, multifactor authentication, physical security, Picture Archiving and Communication System (PACS), privileged account management (PAM), provisioning management, user analytics, vendor neutral archive (VNA).

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology or the National Cybersecurity Center of Excellence, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Table of Contents

1 EXECUTIVE SUMMARY

Purpose

The purpose of this project is to provide guidance and a referenceable architecture for securing the Picture Archiving and Communication System (PACS) ecosystem in Healthcare Delivery Organizations (HDOs), and to include an example solution using existing, commercially and open-source available cybersecurity products.

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. Its hardware components may include workstations, digitizers, communications devices, computers, video monitors, magnetic, optical disk, or other digital data storage devices, and hardcopy devices. The software components may provide functions for performing operations related to image manipulation, enhancement, compression or quantification" [1].

PACS is nearly ubiquitous in hospitals, prompting the National Cybersecurity Center of Excellence (NCCoE) Healthcare Sector Community of Interest to identify securing PACS as a critical need. PACS ties into doctor-patient workflow management, where results based on image interpretation determine the patient's next steps (e.g., determination of health condition, follow-on visits, patient care, other actions). PACS is typically found in image-intensive areas of healthcare (e.g., Radiology, Cardiology, Orthopedics, Pathology, Ophthalmology). Although the PACS fundamentals across clinical disciplines are similar, there are several significant differences due to varying clinical requirements. Therefore, PACS requires controls that provide significant integrity, availability, and confidentiality assurances.

PACS allows for remote image review by users from within the HDO infrastructure and external to the HDO infrastructure. PACS typically interacts with electronic health records (EHRs); Hospital Information System (HIS); Radiology or Cardiology Information System (RIS/CIS); diagnostic reporting; vendor neutral archive (VNA); regulatory registries; and multicenter government, academic, and commercial archives. Users access PACS by using HDO-supplied and configured devices, and personal devices. The amorphous aspect of PACS exposes a threat vector that could act as a point where an attack may be performed or may serve as a pivot point into an integrated healthcare information system.

Compromises on PACS could result in significant data loss, could serve as an avenue to cause disruption throughout a hospital's system, or, should information be altered or misdirected, could impede timely diagnosis and treatment. As healthcare organizations become more-attractive targets for malicious actors, the need to improve these organizations' cybersecurity capabilities is paramount.

Many HDOs face challenges with securing a PACS, including the challenges listed below.

- controlling and monitoring (and auditing) HDO user accounts, including identifying outliers in behavior

- controlling and monitoring (and auditing) access by users that are external to the HDO, including identifying outliers in behavior that are controlling and monitoring (and auditing) access and modification to images
- enforcing least privilege and separation-of-duties policies for all (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

The publication of this Project Description is the beginning of a process that will identify project collaborators, as well as standards-based, commercially and open-source available hardware and software components. These products will be integrated and implemented in a laboratory environment to build open, standards-based, modular, end-to-end reference designs that will address the security challenges of a PACS ecosystem. The approach includes an architectural definition, logical design, build development, security analysis, test and evaluation, security control mapping, and future build considerations. The output of the process will be the publication of a multi-volume National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide that will help healthcare sector organizations implement more-secure PACS solutions through the use of stronger security controls.

The project will use NIST Special Publication (SP) 800-160, Systems Security Engineering, to develop an example solution for securing PACS, and will incorporate the principles of systems security engineering, along with associated activities (i.e., techniques, methods, and practices), into the Practice Guide to ensure that, when used by the targeted audience, the protection needs of stakeholders (i.e., the HDOs) are addressed with the appropriate fidelity and rigor across the entire life cycle of a PACS implementation.

The PACS example solution and Practice Guide will be cognizant of the federal regulations for protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, as described in NIST SP 800-171 Revision 1 [2]. Certain healthcare-related information (e.g., Protected Health Information [PHI]) is considered to be CUI, based on the Security Rule and Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) [3] and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) [4]. The security requirements of NIST SP 800-171 Revision 1 apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. NIST SP 800-171 was established primarily as guidance for the federal community, including contractors and vendors; at a minimum, its content serves as a best-practices guide for HDOs. These security requirements may be referenced in federal contracts involving healthcare and healthcare systems, such as PACS.

Each applicable component of the PACS example solution will be configured to meet the NIST SP 800-171 Revision 1 CUI security requirements, to the extent possible, as supported by the individual vendor products used.

The Practice Guide will include the definition of organizational personnel roles and responsibilities. The project will use the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST SP 800-181) [5] for the following purposes:

- to develop cybersecurity roles and responsibilities applicable to PACS in small, medium, and large HDO environments as well as in individual medical offices
- to specify the knowledge, skills, and abilities required of these defined roles

Scope

The scope of the project will include the PACS ecosystem to allow for the storage, retrieval, management, distribution, and presentation of medical images. The resulting example solution will include implementation of the following items:

- PACS server and archive
- PACS workstation / Digital Imaging and Communications in Medicine (DICOM) viewer
- VNA
- EHR / Electronic Medical Record (EMR) system cloud services
- users with permission to view images
- users with permission to add data to images' activity logging (textual and video)
- typical administrative users

Although the cross-enterprise image-sharing solutions (network-based and CD/DVD-based), for export to and import from other PACS in other sites, are important, the main focus of this project will be limited to address the cybersecurity challenges for the PACS ecosystem within an enterprise.

The Practice Guide will identify which components of the reference architecture are regulated and which are not, based on the vendor filing with the FDA. Understanding the regulated envelope is important, as it defines where HDOs may have flexibility to implement security technologies and measures.

Assumptions

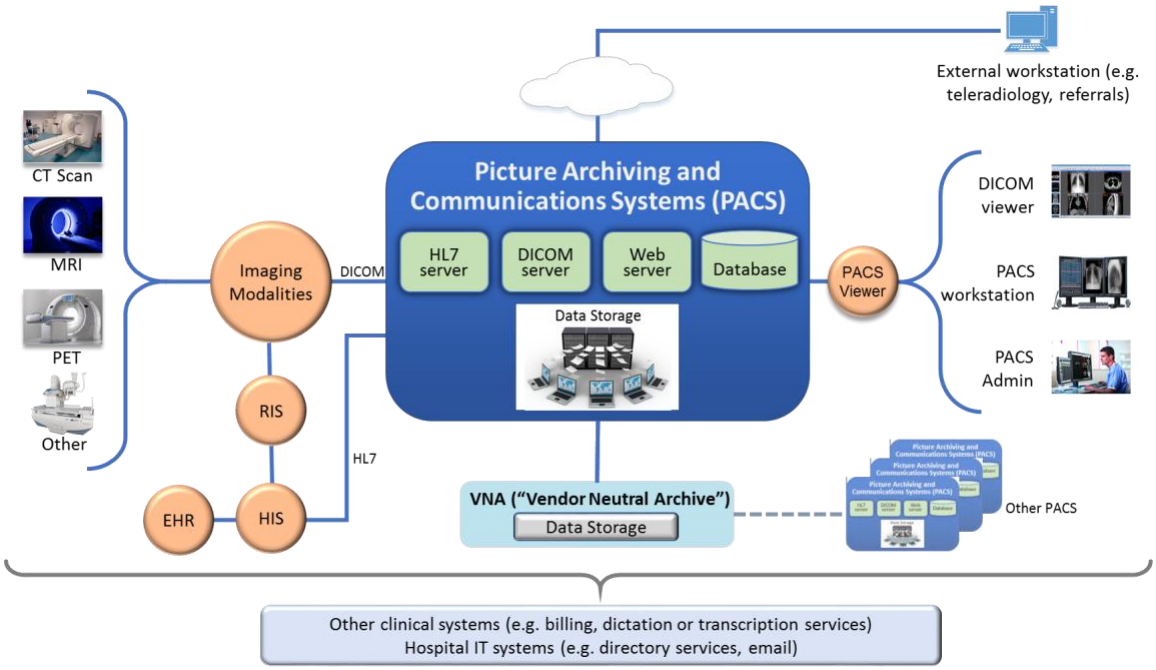
The example solution will use PACS and other components to provide increased security and privacy benefits, while minimizing impacts to availability. The NCCoE assumes that organizations will perform a risk assessment to determine the risk reduction value of an investment in one or more of the PACS capabilities that are included in the reference architecture.

A key assumption is that all potential adopters of this project, or of any of its components, have policies describing the separation of duties and least privilege for administrative/privileged users.

2 HIGH-LEVEL ARCHITECTURE

Figure 2-1 shows the high-level architecture diagram of a representative PACS ecosystem. The reference architecture addresses the scope noted in Section 1, and the desired characteristics noted below. Distinct components will be isolated on the network such that they do not reside on the same Internet Protocol (IP) network. For example, DICOM viewers and PACS workstations may operate in networks that support clinical services; modalities may be deployed to separate medical device zones that prevent inherent trust per medical device zone; PACS web and application servers may be deployed to segregated clinical De-Militarized Zones (DMZs), separate from the core components of the PACS, and segregated from production DMZ demarcations. As appropriate and as may be implemented, components within the PACS may be tiered as well.

Figure 2-1: 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, those listed below.

- PACS servers, special applications (including web services), and workstations
- VNA
- data storage
- modality or modality simulator
- RIS or RIS simulator
- notification system
- EHR/EMR
- 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

Desired Security Characteristics

The security capabilities, behaviors, and life-cycle security requirements of the solution are identified in the list below. Security Capability and Intrinsic Behaviors, and Life Cycle Security are two of the major design principles described in [6].

PACS is a core component in the medical imaging ecosystem, and involves maintaining clinical images used for patient encounter diagnostics and medical history archival. The intent in devising appropriate security measures is to increase security assurance across the HDO enterprise.

The security and privacy controls foundation to be implemented is rooted in the NIST Risk Management Framework, and incorporates elements from Federal Information Processing Standard (FIPS) 199 [7] and 200 [8]; NIST SP 800-60 Revision 1 [9], 800-53 Revision 4 [10], 800-34 Revision 1 [11], and 800-63-3 [12]; and Integrating the Healthcare Enterprise (IHE) practices. The primary security functions and processes to be implemented for this project are listed below and are based on the NIST Cybersecurity Framework (CSF):

IDENTIFY (ID)

- **Asset Management** – includes identification of assets on the network, and management of the assets to be deployed to workstations
- **Risk Assessment** – includes the risk management strategy

PROTECT (PR)

- **Access Control** – includes user account management, remote access
    - controlling (and auditing) user accounts
    - controlling (and auditing) access by external users
    - enforcing least privilege for all (internal and external) users
    - enforcing separation-of-duties policies
        - Privileged Access Management (PAM) with an emphasis on the segregation of duties
    - enforcing least functionality
- **User Identification and Authentication**
    - multifactor authentication for the system that aligns with the sensitive information and function that PACS performs: NIST-recommended algorithms; usability; impact on system performance; and raising the assurance profile, and higher NIST SP 800-63-3 levels, bring a higher level of assurance
    - viable federated identity management
    - credential management
- **Data Security and Privacy** – includes data confidentiality, integrity, and availability
    - securing and monitoring the storage of data – includes data encryption (for data at rest)
        - access control on data
        - data-at-rest controls should implement some form of a data security manager that would allow for policy application to encrypted data, inclusive of access control policy
    - securing the distribution of data – includes data encryption (for data in transit) and a data loss prevention mechanism
    - controls that promote data integrity
    - cryptographic modules validated as meeting NIST FIPS 140-2 are preferred
    - physical security provided by an access controlled data center to host the PACS servers and storage
- **Information Protection Processes and Procedures** – includes data backup, endpoint protection for workstations
- **Maintenance** – local and remote maintenance
- **Protective Technology** – host-based intrusion prevention, solutions for malware (malicious-code detection), audit logging, (automated) audit log review, and physical protection
- **Communications and Network Security** – communications and control networks are protected (e.g., firewall, network access control, network infrastructure controls)
    - securing and monitoring connections within the HDO ecosystem
        - network segmentation
    - securing and monitoring connections to and from external systems

DETECT (DE)

- **Anomalies and Events Detection** – analysis of detected events (from logs, monitoring results, SIEM)
    - centralized mechanism to capture and analyze system and network events
- **Security Continuous Monitoring** – monitoring for unauthorized personnel, devices, software, connections
    - vulnerability management – includes vulnerability scanning and remediation
    - patch management
    - system configuration security settings
    - user account usage (local and remote) and user behavioral analytics

RESPOND (RS)

- **Response Planning** – response plan executed after an event, mitigation of security issues

RECOVER (RC)

- **Recovery and Restoration** – recovery and restoration activities executed after an event
    - business continuity and business resumption processes
        - In addition to a restoration capability from archival media, the project should consider high availability and continuity for data storage. Implicitly, disk arrays used for image storage should have the capability to implement various Redundant Array of Independent Disks (RAID) configurations. RAID 0, 1, 5, 6, and 1+0 should be supported. Disk arrays should also be made available for cold or warm restore/failover capability. Other data storage solutions that provide the same (or better) reliability and durability are considered.

3 SCENARIOS

The following scenarios have been used to develop this project description. IHE Radiology Profiles were referenced for some of the scenarios [13]; they will become the use cases for the design of the reference architecture. Most scenarios emphasize supporting typical workflows or use cases for using the PACS and the medical imaging ecosystem. While the reference architecture needs to ensure that the normal workflow or data flow can accommodate all necessary steps for completing the task, it is important to realize that the reference architecture also needs to ensure that relevant cybersecurity concerns are being addressed for each scenario.

Scenario 1: Sample Radiology Practice Workflows

This scenario covers a few basic workflows:

- order exam for a patient
- post-process images by healthcare professionals
- interpret images and reporting by healthcare professionals

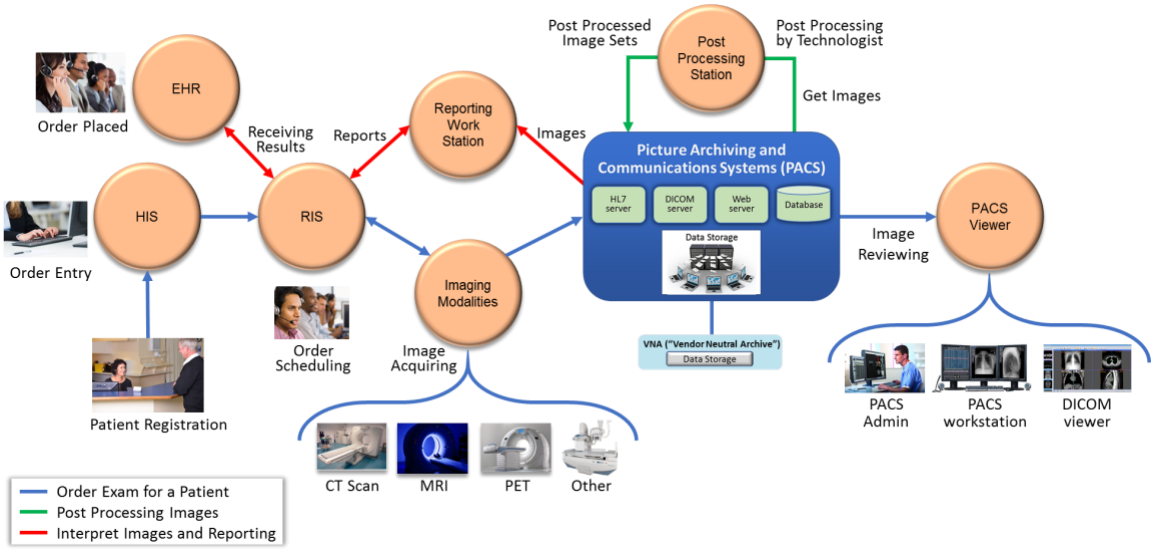
Order Exam for a Patient: This workflow considers a common patient encounter, wherein a patient may be registered within the care provider's systems and a physician requests an image. The patient is scheduled for the imaging activity, the image is acquired, and then the image is routed to a system for storage, viewing and review, and subsequent archival as part of the patient's medical history.

Post-Processing Images: This workflow may involve imaging technologists who may update or monitor the procedure status and capture statistical information pertaining to the image, and generate annotations that are then pushed to the PACS for subsequent workflow triage.

Interpret Images and Reporting: Once the image post-processing is done, healthcare professionals perform analysis, interpretation, and diagnosis with annotations that are pushed to PACS for reporting.

The workflows are depicted in Figure 3-1 below.

Figure 3-1: Sample Radiology Practice Workflows



Note: For purposes of the NCCoE lab environment, several components would be simulated, rather than deploying and using actual equipment. Examples of the use of simulators would be imaging modalities, where the intent would be to generate DICOM and non-DICOM images that are analogous to data that is generated by those devices, short of implementing medical imaging equipment, given that actual deployment may be impractical. A DICOM validation tool can also be used.

The cybersecurity concerns related to this scenario are listed below.

- asset management
- risk assessment
- access control
- user identification and authentication

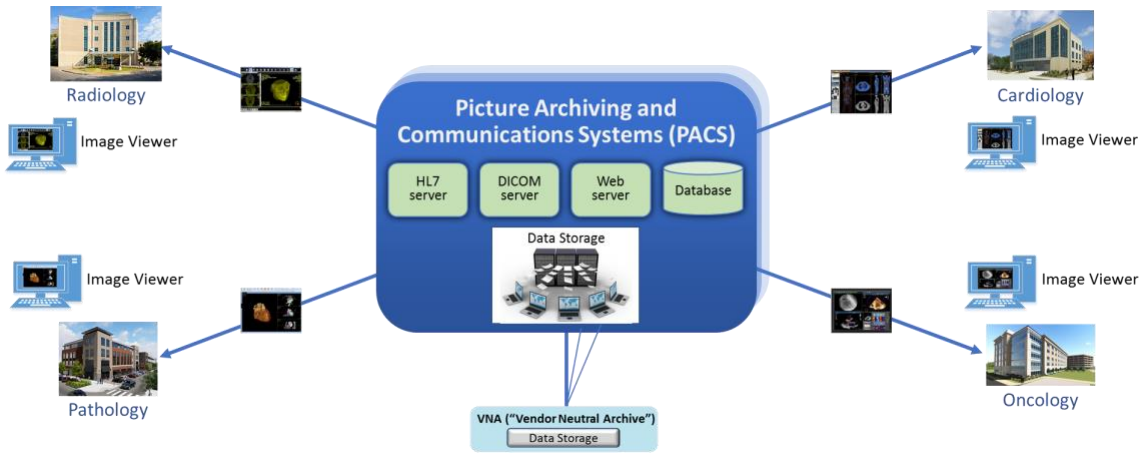
- data security and privacy
- information protection processes and procedures
- maintenance
- protective technology
- communications and network security
- anomalies and events detection
- security continuous monitoring
- response planning
- recovery and restoration

Scenario 2: Image Data Access Across the Enterprise

A collection of medical images and related reports can be aggregated, archived, and accessed by multiple departments within the HDO, such as pathology, surgery, and oncology. The scenario considers the multiple PACS, along with a central VNA and authoritative for cross-departmental imaging. The display function provides consolidated access to additional clinically relevant data from other archives (e.g., Cardiology PACS, long-term archive).

Figure 3-2 shows the arrangement of PACS components planned for the Scenario 2.

Figure 3-2: Image Data Access Across the Enterprise



The cybersecurity concerns related to this scenario are listed below.

- access control
- user identification and authentication
- data security and privacy
- information protection processes and procedures
- protective technology
- communications and network security
- anomalies and events detection

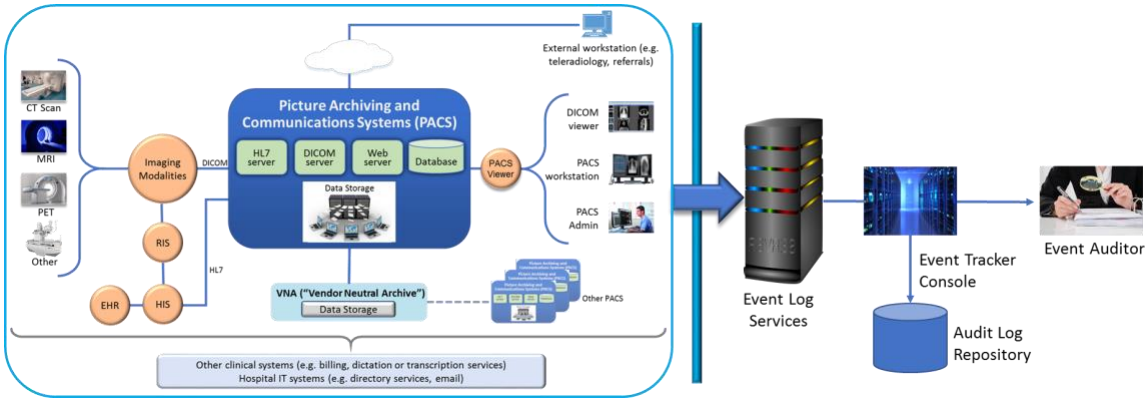
- security continuous monitoring
- response planning
- recovery and restoration

Scenario 3: Accessing, Monitoring, and Auditing

This scenario ensures a centralized and consolidated audit events trail on user and application activity and across several imaging and information systems throughout the enterprise systems that are interconnected in a secure manner. Audit log records will be collected in a repository and will be analyzed by automated means or manually, or by both means.

Figure 3-3 depicts the flow of event and audit data from a PACS environment to the audit log repository, including the analysis of repository data.

Figure 3-3: Accessing, Monitoring, and Auditing



The cybersecurity concerns related to this scenario are listed below.

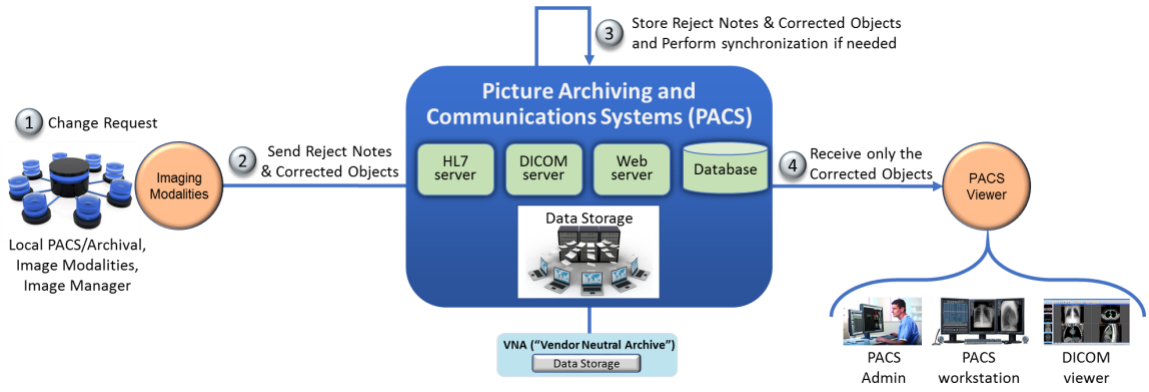
- access control
- user identification and authentication
- data security and privacy
- protective technology
- communications and network security
- anomalies and events detection
- security continuous monitoring

Scenario 4: Imaging Object Change Management

This scenario 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. This scenario defines how changes are captured and how to communicate the changes. This scenario considers those actions when an authorized healthcare professional, upon review of the image, determines that errors or a qualitative defect found in an image may lead to an inappropriate conclusion. The reference architecture needs to ensure that only authorized imaging changes are allowed.

Figure 3-4 shows the data flow involved for the management of changes to imaging objects.

Figure 3-4: Imaging Object Change Management



The cybersecurity concerns related to this scenario are listed below.

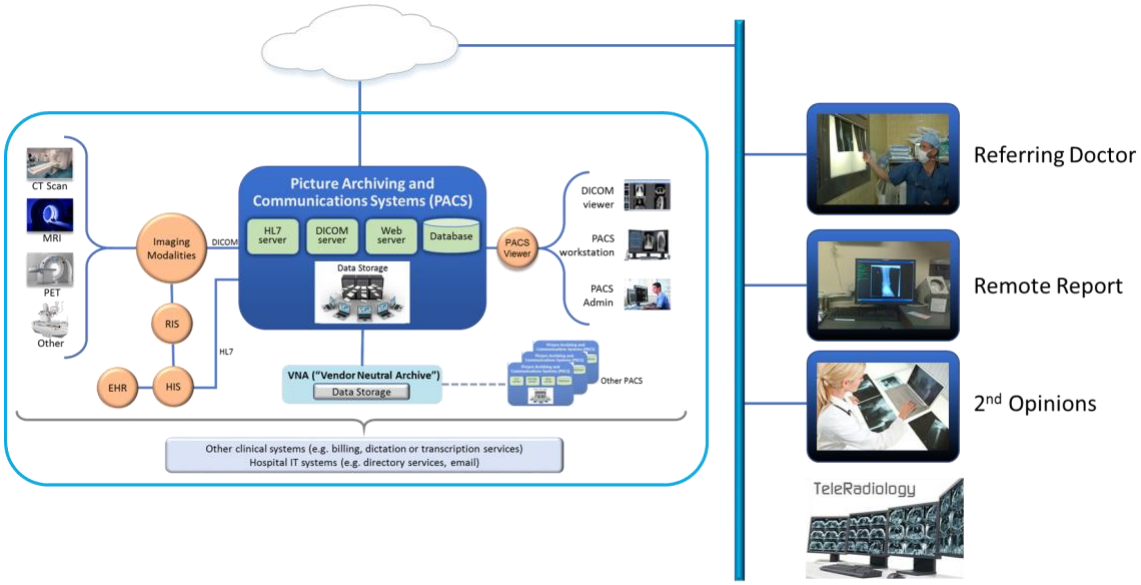
- access control
- user identification and authentication
- data security and privacy
- information protection processes and procedures
- protective technology
- communications and network security
- anomalies and events detection
- security continuous monitoring
- response planning
- recovery and restoration

Scenario 5: Remote Access

Remote access to PACS will be supported, including teleradiology services, which are "now embedded into the workflow of many radiology practices in the United States, driven largely by an expanding corporate model of services" [14]. This scenario supports the means of remote access and considers those actions when authorized healthcare professionals access the required system components. The reference architecture needs to ensure that the same level of safeguarding of the PACS ecosystem is applied for off-hours or overflow reading for another outside facility.

Figure 3-5 presents the Scenario 5 architecture, which supports remote user access.

Figure 3-5: Remote Access



The cybersecurity concerns related to this scenario are listed below.

- access control
- user identification and authentication
- data security and privacy
- information protection processes and procedures
- maintenance
- protective technology
- communications and network security
- anomalies and events detection
- security continuous monitoring
- response planning
- recovery and restoration

4 RELEVANT STANDARDS AND GUIDANCE

General Cybersecurity and Risk Management:

- NIST Cybersecurity Framework
  http://www.nist.gov/itl/cyberframework.cfm
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- ANSI/AAMI/IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices – Part 1: Roles, responsibilities and activities
- IEC Technical Report (TR) 80001-2-1, Edition 1.0 2012-07, Technical Report, Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
- IEC TR 80001-2-2, Edition 1.0 2012-07, Technical Report, Application of risk management for IT Networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- AAMI TIR57, Principles for medical device security – risk management

Cybersecurity / Technology-Related Standards:

- NIST Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules
  https://csrc.nist.gov/publications/detail/fips/140/2/final
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
- NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
- NIST SP 800-57 Part 1 Revision 4 - Recommendation for Key Management: Part 1 – General
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-63-3, Digital Identity Guidelines
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

- NIST SP 800-77, Guide to IPsec VPNs
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf
- NIST SP 800-95, Guide to Secure Web Services
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf
- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
- NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, Security Architecture for the Internet Protocol
  https://tools.ietf.org/html/rfc4301

Other Relevant Regulations, Standards, and Guidance (Healthcare / Medical Devices):

- FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014
  https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
- FDA, Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, Document Issued on: December 28, 2016
  https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf
- FDA, Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf
- FDA, Guidance for Submission of Premarket Notifications for Medical Image Management Devices
  https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm073721.pdf
- FDA, Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Device
  https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm401996.pdf

- NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
- DHHS Office for Civil Rights, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework
  https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
- Department of Homeland Security (DHS), Attack Surface: Healthcare and Public Health Sector
  https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf
- IHE Radiology (RAD) Technical Framework
  http://www.ihe.net/Technical_Frameworks/#radiology
- Digital Imaging and Communications in Medicine (DICOM)
  https://www.dicomstandard.org
- ISO 12052:2011, Health informatics – Digital imaging and communication in medicine (DICOM) including workflow and data management

5 Security Control Map

Table 5-1 maps the characteristics of commercial and open-source products that the NCCoE will apply to this cybersecurity challenge, to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (i.e., CSF), and the Healthcare-Sector-specific standards and guidance, such as International Electrotechnical Commission Technical Report (IEC TR) 80001-2-2, HIPAA, and International Standards Organization / International Electrotechnical Commission (ISO/IEC) 27001. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 5-1: Security Control Map

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53R4**	**IEC TR 80001-2-2**	**HIPAA Security Rule 45**	**ISO/IEC 27001**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	N/A	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
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	RDMP	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	A.12.6.1, A.18.2.3
		ID.RA-4: Potential business impacts and likelihoods are identified	RA-2, RA-3, PM-9, PM-11, SA-14	SAHD, SGUD	C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)	A.12.6.1, A.18.2.3
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2, RA-3, PM-16	SGUD	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.316(a)	None

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53R4**	**IEC TR 80001-2-2**	**HIPAA Security Rule 45**	**ISO/IEC 27001**
		ID.RA-6: Risk responses are identified and prioritized	PM-4, PM-9	DTBK, SGUD	C.F.R. §§ 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)	None
PROTECT (PR)	Identity Management and Access Control (PR.AC)	(Note: not directly mapped in CSF)	AC-1, AC-11, AC-12	ALOF		
		PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	AC-2, IA Family	AUTH, CNFS, EMRG, PAUT	C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	PLOK, TXCF, TXIG	C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	NAUT, PAUT	C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)	A.6.2.2, A.13.1.1, A.13.2.1

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	AUTH, CNFS, EMRG, NAUT, PAUT	C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7	NAUT	C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312€	A.13.1.1, A.13.1.3, A.13.2.1
		PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	AC-2, AC-3, AC-5, AC-6, AC-16, AC-19, AC-24, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	AUTH, CNFS, EMRG, NAUT, PLOK, SGUD,	Not available	A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4
	Data Security (PR.DS)	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

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16		C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)	A.12.3.1
		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5	AUDT, DTBK	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)	A.12.3.1
		PR.DS-5: Protections against data leaks are implemented	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	AUTH, CNFS, STCF, TXCF, TXIG	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312€	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	IGAU	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
		PR.DS-7: The development and testing environment(s) are separate from the production environment	CM-2	CNFS	C.F.R. §§ 164.308(a)(4)4	A.12.1.4

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53R4**	**IEC TR 80001-2-2**	**HIPAA Security Rule 45**	**ISO/IEC 27001**
	Information Protection Processes and Procedures (PR.IP)	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	CP-4, CP-6, CP-9	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
		PR.IP-6: Data is destroyed according to policy	MP-6	DIDT	C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, IR-8	DTBK	C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)	A.16.1.1, A.17.1.1, A.17.1.2
		PR.IP-10: Response and recovery plans are tested	CP-4, IR-3, PM-14	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(D)	A.17.1.3
		PR.IP-12: A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2	MLDP	C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)	A.12.6.1, A.18.2.2
	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-2, MA-3, MA-5	CSUP, RDMP	C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)	A.11.1.2, A.11.2.4, A.11.2.5

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53R4**	**IEC TR 80001-2-2**	**HIPAA Security Rule 45**	**ISO/IEC 27001**
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4	CSUP	C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)	A.11.2.4, A.15.1.1, A.15.2.1
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AC-4, AC-17, AC-18, CP-8, SC-7	AUDT	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	AC-3, CM-7	AUTH, CNFS	C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	A.9.1.2
		PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7	DTBK	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312€	A.13.1.1, A.13.2.1
DETECT (DE)	Anomalies and Events (DE.AE)	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

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	CP-2, IR-4, RA-3, SI -4	DTBK	C.F.R. §§ 164.308(6)(i)	A.16.1.1, A.16.1.4
	Security Continuous Monitoring (DE.CM)	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
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20	MLDP	C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)	None
		DE.CM-4: Malicious code is detected	SI-3	IGAU, MLDP, TXIG	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.2.1
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	RDMP	C.F.R. §§ 164.308(a)(1)(ii)(D)	A.14.2.7, A.15.2.1
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	AUDT, CNFS, PAUT, PLOK, MLDP, NAUT, SGUD	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)	None

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45	ISO/IEC 27001
		DE.CM-8: Vulnerability scans are performed	RA-5	MLDP	C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)	A.12.6.1
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an event	CP-2, CP-10, IR-4, IR-8	DTBK, SGUD, MLDP	C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)	A.16.1.5
	Improvements (RS.IM)	RS.IM-1: Response plans incorporate lessons learned	CP-2, IR-4, IR-8	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))	A.16.1.6
		RS.IM-2: Response strategies are updated	CP-2, IR-4, IR-8	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)	None
RECOVER (RC)	Recovery Planning (RC.RP)	RC.RP-1: Recovery plan is executed during or after an event	CP-10, IR-4, IR-8	DTBK	C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)	A.16.1.5

APPENDIX A – REFERENCES

[1] Food and Drug Administration, "Display Devices for Diagnostic, Guidance for Industry and Food and Drug Administration Staff," Food and Drug Administration, 2017.

[2] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey and M. Riddle, December 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[3] 104th Congress, "Health Insurance Potability and Accountability Act of 1996," 1996 August 21. [Online]. Available: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996.

[4] Congress, "Health Information Technology for Economic and Clinical Health Act (HITECH)," 17 February 2009. [Online]. Available: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

[5] W. Newhouse, S. Keith, B. Scribner and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[6] R. Ross, M. McEvilley and J. Oren, Special Publication 800-160, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Gaithersburg, MD: National Institute of Standards and Technology, 2016.

[7] National Institutes of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[8] National Institutes of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems," March 2006. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[9] K. Stine, R. Kissel, W. C. Barker, J. Fahlsing and J. Gulick, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

[10] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[11] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup and D. Lynes, "Contingency Planning Guide for Federal Information Systems," May 2010. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

[12] P. A. Grassi, M. E. Garcia and J. L. Fenton, "Digital Identity Guidelines," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html.

[13] Integrating the Healthcare Enterprise (IHE), [Online]. Available: http://wiki.ihe.net/index.php/Profiles - IHE_Radiology_Profiles.

[14] E. Silva III, J. Breslau, L. A. Liebscher, M. Bohl, T. Hoffman, G. W. L. Boland, C. Sherry, W. Kim, S. S. Shah and M. Tilkin, "ACR White Paper on Teleradiology Practice: A Report From the Task Force on Teleradiology Practice," *Journal of the American College of Radiology,* vol. 10, no. 8, pp. 575 - 585, 2013.