

Regulatory Requirements for PACS Systems

ADA Compliance – Federal standards ensuring accessibility of PACS interfaces for individuals with disabilities. Related terms: 508, WCAG. Example: Keyboard-only navigation for image review. Challenge: Balancing usability with strict accessibility guidelines.

Adverse Event Reporting – Mandatory submission of incidents where PACS malfunction leads to patient harm. Related terms: FDA, MAUDE. Example: Incorrect image labeling causing diagnostic error. Challenge: Timely detection and accurate root-cause analysis.

AFR (Annual Facility Review) – Yearly audit of PACD (PACS Diagnostic) infrastructure against regulatory benchmarks. Related terms: QC, CAP. Example: Verifying backup storage capacity meets 30-day retention. Challenge: Coordinating multidisciplinary teams within limited windows.

AHIMA Guidelines – Best-practice recommendations from the American Health Information Management Association for imaging data stewardship. Related terms: HIPAA, NIST. Example: Defining role-based access for radiology technologists. Challenge: Translating broad guidance into site-specific policies.

AI/ML Validation – Process of confirming that artificial intelligence tools integrated with PACS meet safety and efficacy standards. Related terms: FDA 510(k), SaMD. Example: Validating a deep-learning algorithm for lung nodule detection. Challenge: Maintaining continuous performance monitoring as data drift occurs.

ALARA Principle – “As Low As Reasonably Achievable” concept applied to radiation exposure and also to data handling overhead. Related terms: DRL, dose optimization. Example: Configuring automatic exposure control to reduce repeat scans. Challenge: Ensuring image quality remains diagnostic while minimizing dose.

AMC (Accreditation Management Council) – Body that oversees compliance of imaging departments with national accreditation standards. Related terms: JCAHO, ISO. Example: Preparing for an on-site audit of PACS workflow documentation. Challenge: Aligning internal SOPs with evolving accreditation criteria.

ANSI Standards – Technical specifications from the American National Standards Institute relevant to medical imaging data formats. Related terms: DICOM, HL7. Example: Implementing DICOM-SR for structured reporting. Challenge: Keeping implementations up-to-date with periodic revisions.

APIs (Application Programming Interfaces) – Defined methods for external systems to interact with PACS, subject to security and interoperability regulations. Related terms: FHIR, REST. Example: Using an API to retrieve study metadata for research. Challenge: Managing version control and authentication across multiple vendors.

ARC (Archive Retention Compliance) – Requirement to retain imaging studies for a specified period, often 5–10 years, depending on jurisdiction. Related terms: GDPR, HIPAA. Example: Configuring tiered storage to

meet 7-year retention for oncology patients. Challenge: Balancing storage cost with legal obligations.

ASLR (Address Space Layout Randomization) – Security technique to randomize memory addresses, mitigating exploitation of PACS server vulnerabilities. Related terms: OS hardening, SELinux. Example: Enabling ASLR on Linux-based image archive nodes. Challenge: Ensuring compatibility with legacy imaging software that assumes static memory locations.

Audit Trail – Immutable log of user actions within PACS, required for forensic analysis and regulatory compliance. Related terms: Log management, SIEM. Example: Recording every image view, export, and deletion event. Challenge: Storing high-volume logs without impacting system performance.

AVC (Audit Validation Criteria) – Set of metrics used to assess the completeness and accuracy of audit logs. Related terms: NIST SP 800-92, SOC2. Example: Verifying that timestamps are synchronized to NTP servers. Challenge: Detecting and correcting clock drift across distributed nodes.

BCP (Business Continuity Plan) – Documented strategy to maintain PACS operations during disruptions. Related terms: DR, RPO. Example: Switching to a hot-standby archive site after a power outage. Challenge: Regularly testing failover without affecting clinical workflow.

CAPA (Corrective and Preventive Action) – Structured approach to address identified non-conformities in PACS processes. Related terms: Root cause analysis, QMS. Example: Updating firmware after a recurring network timeout error. Challenge: Tracking effectiveness of implemented actions over time.

CCPA (California Consumer Privacy Act) – State-level privacy law influencing how patient imaging data is stored and shared. Example: Providing patients with the right to request deletion of their images. Challenge: Reconciling CCPA deletion requests with mandatory retention periods.

CDR (Clinical Data Repository) – Centralized database that aggregates imaging metadata for research and quality improvement. Related terms: Data warehouse, ETL. Example: Exporting structured DICOM tags to a CDR for outcome studies. Challenge: Ensuring de-identification complies with privacy statutes.

CE Marking – European conformity label indicating that PACS equipment meets essential health-safety requirements. Related terms: MDR, EU Directives. Example: Certifying a new workstation as CE-marked before deployment in the EU. Challenge: Maintaining documentation for ongoing post-market surveillance.

CHIP (Certified Health Imaging Professional) – Credential demonstrating expertise in PACS operation and regulatory compliance. Related terms: RHIA, RIT. Example: A PACS analyst obtaining CHIP certification to lead an audit. Challenge: Keeping certification current amid rapid technology changes.

CHOP (Clinical Health Operations Protocol) – Institution-specific set of procedures governing image acquisition, storage, and distribution. Related terms: SOP, workflow. Example: Defining the sequence for image archiving after a CT scan. Challenge: Aligning CHOP with external standards without creating redundancy.

CIS (Critical Infrastructure Security) – Framework addressing protection of essential medical imaging services against cyber threats. Related terms: NIST CSF, IEC 62443. Example: Implementing network

segmentation for PACS servers. Challenge: Balancing security controls with the need for rapid image access.

CLIA (Clinical Laboratory Improvement Amendments) – Federal regulation that, while primarily for labs, also impacts image-based diagnostics. Related terms: CAP, FDA. Example: Validating image analysis software used for pathology slide interpretation. Challenge: Demonstrating analytical validity for imaging assays.

CMR (Change Management Request) – Formal proposal to modify PACS configuration, hardware, or software, requiring risk assessment. Related terms: ITIL, RFC. Example: Requesting additional storage nodes to support higher study volumes. Challenge: Obtaining timely approvals while maintaining compliance documentation.

COBIT (Control Objectives for Information and Related Technologies) – Governance framework that can be applied to PACS governance and risk management. Related terms: ITIL, ISO 27001. Example: Mapping PACS security controls to COBIT's DSS04 objective. Challenge: Tailoring generic controls to the specific nuances of imaging data.

CMOS (Clinical Management of Operating Systems) – Policies governing the operating system environment of PACS workstations and servers. Related terms: Patch management, OS hardening. Example: Enforcing quarterly security patches on Windows 10 imaging consoles. Challenge: Avoiding downtime during patch cycles that could delay clinical reads.

COA (Certificate of Authorization) – Document granting permission to operate a PACS system in a specific jurisdiction, often required for cross-border data exchange. Related terms: Data sharing agreement, MOU. Example: Securing a COA before enabling tele-radiology services between Canada and the U.S. Challenge: Coordinating differing regulatory timelines across agencies.

CRF (Case Report Form) – Structured document used in clinical trials that may incorporate imaging endpoints captured by PACS. Related terms: eCRF, GCP. Example: Populating a CRF with tumor measurement data extracted from DICOM SR. Challenge: Ensuring data integrity when integrating PACS outputs into trial databases.

CRL (Certificate Revocation List) – List of digital certificates that have been revoked, used to maintain trust in PACS communication channels. Related terms: PKI, TLS. Example: Updating PACS servers to check the latest CRL for client certificates. Challenge: Managing timely distribution of revocation information across a distributed network.

CSA (Cloud Service Assurance) – Set of standards for evaluating the security and compliance of cloud-based PACS solutions. Related terms: ISO 27017, SOC 2. Example: Conducting a CSA audit before migrating archival storage to a public cloud. Challenge: Mapping cloud provider controls to internal regulatory requirements.

CTP (Clinical Trial Protocol) – Document outlining imaging requirements for a study, referencing PACS capabilities and compliance obligations. Related terms: IRB, GCP. Example: Defining image acquisition parameters and storage duration in the CTP. Challenge: Aligning protocol specifications with existing PACS configurations without extensive re-engineering.

CTR (Clinical Trial Registration) – Process of publicly listing a trial, including imaging endpoints that must comply with data-privacy regulations. Related terms: FDAAA, WHO ICTRP. Example: Registering a trial that uses PACS-derived biomarkers. Challenge: Maintaining consistent data standards across multiple trial sites.

CTDS (Computed Tomography Dose Surveillance) – Program monitoring CT dose metrics, often integrated with PACS for dose reporting. Related terms: DRL, DICOM Dose Report. Example: Automatically populating a dose-tracking dashboard from PACS metadata. Challenge: Ensuring accurate dose capture across diverse scanner models.

DICOM (Digital Imaging and Communications in Medicine) – International standard governing the format and exchange of medical images. Related terms: HL7, IHE. Example: Using DICOM-web services to retrieve studies via RESTful APIs. Challenge: Maintaining compliance with DICOM-PS3 updates while supporting legacy equipment.

DLP (Data Loss Prevention) – Suite of technologies and policies designed to prevent unauthorized disclosure of imaging data. Related terms: Encryption, IDS. Example: Configuring DLP rules to block outbound transmission of unencrypted PHI. Challenge: Reducing false-positive alerts that impede clinical workflow.

DR (Disaster Recovery) – Set of procedures to restore PACS functionality after a catastrophic event. Related terms: BCP, RTO. Example: Restoring image archives from off-site snapshots following a ransomware attack. Challenge: Verifying data integrity of restored studies without interrupting patient care.

DRM (Digital Rights Management) – Controls governing the usage, sharing, and retention of imaging data, often mandated by licensing agreements. Related terms: Access control, watermarking. Example: Restricting export of proprietary research images to authorized users. Challenge: Implementing DRM without degrading image quality for diagnostic interpretation.

DRL (Dose Reference Level) – Benchmark radiation dose used to assess and optimize imaging protocols. Related terms: ALARA, CTDS. Example: Adjusting PACS-linked protocol parameters when a study exceeds the DRL. Challenge: Communicating dose alerts to technologists without causing alert fatigue.

DSGVO (Datenschutz-Grundverordnung) – German term for GDPR, influencing PACS handling of personal health data within the EU. Related terms: GDPR, CE Marking. Example: Implementing a “right to be forgotten” workflow for imaging data. Challenge: Reconciling DSGVO deletion requests with mandatory retention obligations.

ECC (Elliptic Curve Cryptography) – Modern encryption method recommended for securing PACS data in transit and at rest. Related terms: TLS 1.3, PKI. Example: Deploying ECC-based certificates for PACS web portals. Challenge: Ensuring compatibility with older imaging modalities that only support RSA.

EMR (Electronic Medical Record) – Digital health record that often integrates with PACS to provide a unified patient view. Related terms: EHR, HL7. Example: Embedding a PACS viewer within the EMR interface. Challenge: Maintaining data integrity and auditability across disparate systems.

EN ISO 14971 – International standard for risk management of medical devices, applicable to PACS hardware and software. Related terms: FDA 510(k), IEC 62304. Example: Conducting a risk analysis for a new PACS workstation model. Challenge: Documenting risk controls that satisfy both global and local regulators.

EPA (Electronic Protected Access) – Security model that defines tiered authentication mechanisms for PACS users. Related terms: MFA, RBAC. Example: Requiring biometric verification for high-risk image export functions. Challenge: Balancing usability for technologists with stringent access controls.

EPA (Environmental Protection Agency) – Agency whose regulations on electronic waste disposal affect decommissioning of PACS hardware. Related terms: e-waste, RCRA. Example: Recycling obsolete PACS servers according to EPA guidelines. Challenge: Tracking hazardous components while ensuring data sanitization.

FIPS (Federal Information Processing Standards) – Set of U.S. Government standards for cryptographic modules used in PACS. Related terms: NIAP, NIST. Example: Deploying FIPS-validated encryption libraries for image storage. Challenge: Ensuring third-party vendors provide FIPS-certified components.

FHIR (Fast Healthcare Interoperability Resources) – Modern standard for exchanging healthcare data, increasingly used alongside DICOM in PACS ecosystems. Related terms: API, HL7. Example: Querying a FHIR-based patient resource to retrieve associated imaging studies. Challenge: Mapping complex imaging metadata to FHIR resources without loss of fidelity.

GDPR (General Data Protection Regulation) – EU regulation governing processing of personal data, including medical images. Related terms: DSGVO, CCPA. Example: Implementing consent management for cross-border image sharing. Challenge: Maintaining compliance while supporting urgent clinical decision-making.

GxP (Good Practice) – Collective term for quality standards (e.G., GCP, GLP) that extend to imaging data handling in clinical research. Related terms: GCP, SOP. Example: Applying GxP documentation to a PACS validation protocol. Challenge: Aligning GxP requirements with routine clinical operations.

HA (High Availability) – Architectural design ensuring continuous PACS service delivery with minimal downtime. Related terms: Cluster, Load balancing. Example: Deploying active-passive server pairs for image retrieval. Challenge: Synchronizing stateful session data across HA nodes.

HIPAA (Health Insurance Portability and Accountability Act) – U.S. Law defining privacy and security safeguards for protected health information, including imaging data. Related terms: HITECH, NIST. Example: Encrypting DICOM files at rest to meet HIPAA's technical safeguards. Challenge: Conducting periodic risk assessments that capture evolving threats.

HITRUST CSF – Framework that consolidates multiple security and privacy regulations, often adopted by organizations operating PACS. Related terms: ISO 27001, NIST. Example: Mapping PACS controls to the HITRUST CSF to achieve certification. Challenge: Maintaining the comprehensive documentation required for annual assessments.

HL7 (Health Level Seven) – Set of international standards for the exchange of clinical and administrative data, frequently interfaced with PACS. Related terms: FHIR, IHE. Example: Using HL7 ADT messages to trigger study archiving in PACS. Challenge: Coordinating message timing to avoid race conditions with image acquisition.

ICD (International Classification of Diseases) – Coding system that may be linked to imaging studies for billing and research purposes. Related terms: CPT, SNOMED CT. Example: Assigning an ICD-10 code to a radiology report stored in PACS. Challenge: Ensuring accurate code mapping across different clinical vocabularies.

IEC 62304 – Standard for medical device software lifecycle processes, applicable to PACS applications. Related terms: EN ISO 14971, FDA 510(k). Example: Documenting software development phases for a new PACS viewer. Challenge: Aligning agile development practices with the rigorous documentation required by IEC 62304.

IEC 62443 – Series of standards addressing industrial automation and control system security, relevant to PACS network architecture. Related terms: CIS, NIST CSF. Example: Implementing zone-based security zones for imaging modality networks. Challenge: Integrating legacy scanners that lack modern security features.

IFU (Instructions for Use) – Manufacturer-provided documentation that includes regulatory compliance statements for PACS equipment. Related terms: Labeling, CE Marking. Example: Reviewing the IFU to verify required periodic safety checks. Challenge: Updating IFU references when software patches modify functionality.

IAM (Identity and Access Management) – Framework for managing user identities, roles, and permissions within PACS. Related terms: RBAC, MFA. Example: Provisioning a new radiology resident with read-only access to specific study types. Challenge: Synchronizing IAM across on-premise and cloud-based PACS components.

ICD-10-CM – Clinical modification of ICD-10 used for diagnosis coding that can be associated with imaging studies. Related terms: CPT, DRG. Example: Linking a chest X-ray study to the patient's ICD-10-CM code for billing. Challenge: Maintaining accurate code updates as clinical documentation evolves.

IE (Information Exchange) – Formal process of transmitting imaging data between PACS and external systems, governed by standards and regulations. Example: Scheduling a nightly batch export of studies to a regional health information exchange. Challenge: Ensuring encryption and auditability throughout the exchange pipeline.

IEC 60601-2-33 – Safety standard for diagnostic X-ray equipment, influencing PACS compliance when handling such modalities. Related terms: FDA, CE Marking. Example: Verifying that PACS correctly records safety-critical parameters from a CT scanner. Challenge: Coordinating compliance testing across multiple device manufacturers.

ISO 13485 – Quality management system standard for medical device manufacturers, including PACS vendors. Related terms: QMS, CAPA. Example: Auditing a PACS vendor's ISO 13485 certification during

contract renewal. Challenge: Aligning vendor quality audits with internal regulatory timelines.

ISO 27001 – International standard for information security management systems, often adopted for PACS security programs. Related terms: HITRUST, NIST. Example: Conducting an ISO 27001 risk assessment covering image storage encryption. Challenge: Maintaining continuous improvement in the face of emerging threats.

ISO 27799 – Standard providing guidance on health informatics security, directly applicable to PACS data protection. Related terms: ISO 27001, GDPR. Example: Implementing ISO 27799 recommendations for secure image transmission over VPNs. Challenge: Translating high-level controls into operational procedures for radiology staff.

ISO 9001 – General quality management standard that can underpin PACS process improvement initiatives. Related terms: ISO 13485, QMS. Example: Using ISO 9001 process mapping to streamline image archiving workflows. Challenge: Demonstrating relevance of a generic QMS to specialized imaging operations.

ITIL (Information Technology Infrastructure Library) – Framework for IT service management that supports PACS operational excellence. Related terms: CMR, COBIT. Example: Applying ITIL change management to schedule PACS software upgrades. Challenge: Integrating ITIL processes with clinical urgency and turnaround-time expectations.

JCAHO (Joint Commission on Accreditation of Healthcare Organizations) – Accrediting body whose standards include imaging safety and PACS performance. Related terms: AMC, CAP. Example: Preparing for a JCAHO survey that reviews PACS image availability metrics. Challenge: Aligning JCAHO requirements with other regulatory mandates without duplication.

LAN (Local Area Network) – Physical network infrastructure that connects imaging modalities to the PACS server, subject to performance and security standards. Related terms: WAN, VLAN. Example: Configuring a dedicated DICOM VLAN to isolate imaging traffic. Challenge: Managing bandwidth to prevent bottlenecks during high-volume imaging periods.

LEDs (Low-Energy Data Storage) – Emerging storage technology promoting energy-efficient archival of large imaging datasets. Related terms: TCO, Green IT. Example: Migrating older studies to LEDs to reduce data-center power consumption. Challenge: Verifying long-term data integrity and regulatory compliance of new media.

LLR (Long-Term Retention) – Policy specifying the duration for which imaging studies must be kept, often exceeding standard ARC requirements. Related terms: ARC, RPO. Example: Maintaining a 15-year LLR for pediatric oncology studies. Challenge: Scaling storage while ensuring retrieval performance for legacy data.

LOE (Level of Evidence) – Classification of the scientific support for imaging findings, sometimes referenced in PACS reporting tools. Related terms: GRADE, EBM. Example: Tagging a radiology report with LOEB when the finding is based on a prospective cohort study. Challenge: Integrating LOE metadata without disrupting clinical documentation workflows.

MDR (Medical Device Regulation) – EU regulation replacing the Medical Device Directive, governing PACS software classified as a medical device. Related terms: CE Marking, ISO 13485. Example: Conducting a conformity assessment for a new AI-assisted PACS viewer under MDR. Challenge: Managing post-market surveillance obligations across multiple EU member states.

MLP (Minimum Legal Period) – Shortest duration required by law to retain imaging records, varying by jurisdiction. Related terms: ARC, LLR. Example: Retaining emergency department CT scans for at least 5 years per state law. Challenge: Harmonizing MLP with longer internal retention policies without redundant duplication.

MTBF (Mean Time Between Failures) – Reliability metric used to predict PACS hardware longevity and schedule preventive maintenance. Related terms: MTTR, Reliability Engineering. Example: Selecting storage arrays with an MTBF exceeding 150,000 hours for critical archive nodes. Challenge: Translating MTBF data into actionable maintenance intervals.

MTTR (Mean Time To Repair) – Average time required to restore PACS functionality after a failure, a key performance indicator for service level agreements. Related terms: MTBF, SLA. Example: Targeting an MTTR of less than 30 minutes for network-related image retrieval failures. Challenge: Balancing rapid restoration with thorough root-cause documentation.

MFA (Multi-Factor Authentication) – Security measure requiring two or more verification methods before granting PACS access. Related terms: EPA, IAM. Example: Requiring a hardware token plus password for administrators modifying archive settings. Challenge: Ensuring MFA devices are available during on-call emergencies without causing access delays.

ML (Machine Learning) – Subset of AI used to enhance image interpretation, workflow triage, and quality control within PACS. Related terms: AI/ML Validation, SaMD. Example: Deploying a convolutional neural network to flag potential missed fractures. Challenge: Maintaining model performance as imaging protocols evolve.

NSA (National Security Agency) – U.S. Agency whose guidelines influence the cryptographic standards applied to PACS data protection. Related terms: FIPS, NIST. Example: Aligning PACS encryption with NSA's Suite B recommendations. Challenge: Keeping up with evolving NSA cryptographic guidance while avoiding vendor lock-in.

NTLM (NT LAN Manager) – Legacy Microsoft authentication protocol sometimes still used by older PACS workstations, requiring careful security assessment. Related terms: Kerberos, LDAP. Example: Disabling NTLM in favor of Kerberos for all new PACS client connections. Challenge: Migrating legacy devices without disrupting clinical operations.

PCI DSS (Payment Card Industry Data Security Standard) – While primarily for payment data, its controls can inform PACS security practices when billing information is embedded in imaging reports. Related terms: HIPAA, DLP. Example: Applying PCI-style network segmentation to isolate billing-related data flows. Challenge: Avoiding unnecessary compliance overhead while still protecting patient information.

PHI (Protected Health Information) – Any individually identifiable health data, including imaging studies, that must be safeguarded under privacy regulations. Related terms: HIPAA, GDPR. Example: Encrypting PHI in DICOM files both at rest and during transmission. Challenge: Ensuring de-identification processes retain essential diagnostic information.

PKI (Public Key Infrastructure) – Framework for managing digital certificates used to secure PACS communications and authentication. Related terms: CRL, TLS. Example: Issuing client certificates to radiologists for secure VPN access to the PACS archive. Challenge: Rotating certificates before expiration without causing service interruptions.

PM (Preventive Maintenance) – Scheduled activities designed to reduce the likelihood of PACS component failure. Related terms: MTBF, CMOS. Example: Quarterly cleaning of server fans and firmware updates on imaging modality interfaces. Challenge: Coordinating maintenance windows with clinical schedules to avoid impact on patient care.

POC (Proof of Concept) – Early-stage demonstration that a new technology (e.g., AI integration) can work within the PACS environment and meet regulatory criteria. Related terms: Pilot, Validation. Example: Running a POC to assess the feasibility of blockchain-based image provenance tracking. Challenge: Scaling the POC to production while maintaining compliance documentation.

POU (Point of Use) – Location where imaging data is accessed, such as a radiology reading room, requiring localized security controls. Related terms: EPA, RBAC. Example: Enforcing screen-lock timers on POU workstations to protect PHI. Challenge: Balancing strict controls with the need for rapid image manipulation during interpretation.

QoS (Quality of Service) – Network feature that prioritizes DICOM traffic to ensure timely image delivery. Related terms: LAN, VLAN. Example: Configuring QoS rules to give CT scan data higher priority than routine X-ray transfers. Challenge: Monitoring QoS effectiveness without introducing latency for other critical hospital services.

RA (Risk Assessment) EN ISO 14971, NIST SP 800-30. Example: Conducting an RA for a new cloud-based archival solution. Challenge: Keeping the RA current as system components and threat landscapes evolve.

RACI (Responsible, Accountable, Consulted, Informed) – Matrix used to clarify roles in PACS governance and compliance projects. Related terms: SOP, Governance. Example: Assigning “Accountable” status to the Chief Imaging Officer for PACS security policy updates. Challenge: Ensuring all stakeholders understand and adhere to their RACI designations.

RADIUS (Remote Authentication Dial-In User Service) – Protocol for centralized authentication, often employed in PACS network access control. Related terms: MFA, LDAP. Example: Configuring RADIUS to authenticate radiology staff connecting to the PACS VPN. Challenge: Integrating RADIUS with existing Active Directory structures without creating duplicate accounts.

RBAC (Role-Based Access Control) – Access model granting permissions based on user roles, essential for PACS compliance with privacy laws. Related terms: IAM, EPA. Example: Defining a “Technician” role that can

view but not export studies. Challenge: Regularly reviewing role definitions to reflect changing job responsibilities.

RPO (Recovery Point Objective) – Maximum tolerable period of data loss measured in time, critical for PACS disaster recovery planning. Related terms: RTO, DR. Example: Setting an RPO of 4 hours for critical imaging archives. Challenge: Aligning backup frequency with storage cost constraints while meeting clinical continuity needs.

RTO (Recovery Time Objective) – Targeted duration to restore PACS services after an outage, influencing failover architecture. Related terms: RPO, DR. Example: Designing a hot-standby architecture to achieve an RTO of 15 minutes. Challenge: Testing the RTO regularly without disrupting ongoing clinical work.

SA (Security Assessment) – Formal evaluation of PACS controls against regulatory benchmarks and industry best practices. Related terms: NIST, HITRUST. Example: Performing a penetration test on the PACS web interface. Challenge: Addressing identified vulnerabilities while maintaining uninterrupted image access.

SaaS (Software as a Service) – Delivery model where PACS functionality is hosted by a third-party provider, bringing specific regulatory considerations. Related terms: CSA, Cloud. Example: Subscribing to a SaaS-based PACS viewer for remote radiology reads. Challenge: Ensuring the provider's compliance certifications align with institutional policies.

SAML (Security Assertion Markup Language) – Standard for exchanging authentication and authorization data between identity providers and PACS applications. Related terms: SSO, IAM. Example: Implementing SAML-based single sign-on for radiologists accessing multiple imaging systems. Challenge: Mapping SAML attributes to PACS role definitions accurately.

SCP (Secure Copy Protocol) – Method for securely transferring files, occasionally used for moving large imaging datasets between sites. Related terms: SSH, TLS. Example: Automating nightly SCP transfers of de-identified studies to a research server. Challenge: Managing key distribution and ensuring compliance with data-transfer encryption policies.

SDLC (Software Development Life Cycle) – Structured process for developing PACS applications, required to meet regulatory software standards. Related terms: IEC 62304, Agile. Example: Incorporating validation testing at each SDLC phase for a new PACS viewer. Challenge: Reconciling fast-paced agile iterations with extensive documentation mandates.

SE (Software Engineering) – Discipline encompassing design, development, testing, and maintenance of PACS software, governed by regulatory standards. Related terms: SDLC, IEC 62304. Example: Applying static code analysis to detect security flaws in PACS modules. Challenge: Maintaining code quality across multiple development teams and third-party components.

SEC (Security) – Broad term encompassing all protective measures applied to PACS, from physical safeguards to cyber defenses. Related terms: CIS, NIST. Example: Conducting a comprehensive SEC audit covering firewalls, encryption, and access logs. Challenge: Ensuring the SEC program remains proportionate to the risk profile of imaging services.

SIEM (Security Information and Event Management) – Platform aggregating and analyzing logs from PACS components to detect security incidents. Related terms: Audit Trail, IDS. Example: Configuring SIEM alerts for anomalous bulk export of DICOM studies. Challenge: Tuning detection rules to minimize false positives that could interrupt clinical workflow.

SLA (Service Level Agreement) – Contractual document defining performance and availability expectations for PACS services. Related terms: RTO, MTTR. Example: Including a clause that 99.9% Uptime must be maintained for the image archive. Challenge: Negotiating SLA terms that reflect realistic operational capabilities while satisfying clinical stakeholders.

SOX (Sarbanes-Oxley Act) – U.S. Legislation primarily affecting financial reporting, but its internal control requirements can influence PACS governance when imaging data contributes to revenue cycles. Related terms: HIPAA, GxP. Example: Implementing controls to ensure imaging charges are accurately reflected in billing systems. Challenge: Aligning SOX control documentation with medical imaging processes without creating redundant audits.

SP (Standard Procedure) – Documented method for routine PACS tasks, forming part of the quality management system. Related terms: SOP, SOP. Example: An SP for performing weekly integrity checks on archive media. Challenge: Keeping SPs current as software versions and hardware configurations evolve.

SOP (Standard Operating Procedure) – Detailed, step-by-step instructions for performing PACS activities, required for regulatory compliance. Related terms: SP, QMS. Example: SOP outlining the process for anonymizing images before research export. Challenge: Ensuring staff adherence while allowing flexibility for emergency situations.

SPI (Security Parameter Index) – Identifier used in IPsec to manage security associations for encrypted PACS traffic. Related terms: IPsec, VPN. Example: Assigning a unique SPI for each DICOM communication tunnel. Challenge: Managing SPI lifecycle across multiple gateways and ensuring synchronization.

SQL Injection – Attack vector that can compromise PACS databases if input validation is insufficient. Related terms: OWASP, Input Sanitization. Example: Exploiting a vulnerable search field to retrieve unauthorized patient images. Challenge: Implementing robust validation without degrading query performance for radiologists.

SSO (Single Sign-On) – Authentication mechanism allowing users to access multiple PACS components with one credential set. Related terms: SAML, IAM. Example: Enabling SSO so a radiologist can seamlessly move from the viewer to the reporting system. Challenge: Managing session timeouts to prevent unauthorized access after the user leaves the workstation.

TLS (Transport Layer Security) – Protocol providing encrypted communications for PACS data transfers over networks. Related terms: SSL, PKI. Example: Enforcing TLS 1.3 For all DICOMweb requests. Challenge: Ensuring all legacy imaging devices support the selected TLS version.

UAT (User Acceptance Testing) – Final validation phase where end-users verify that PACS functionality meets clinical and regulatory requirements. Related terms: Validation, QA. Example: Radiologists testing a new

annotation tool for compliance with DICOM SR standards. Challenge: Capturing detailed feedback while keeping testing timelines aligned with deployment schedules.