
Global Certificate Course in Healthcare Cybersecurity for Nurses

Fundamentals of Healthcare Cybersecurity

Access Control – Related terms: authentication, authorization, least privilege. A set of policies and mechanisms that limit who can view or use information resources. Example: Role-based access control (RBAC) restricts a nurse's access to patient charts based on job function. Challenge: Balancing security with workflow efficiency to avoid "alert fatigue."

Advanced Persistent Threat (APT) – Related terms: nation-state actors, cyber espionage. A prolonged, targeted cyberattack where attackers remain undetected while extracting data. Example: An APT infiltrates a hospital's EMR system to steal research data. Challenge: Detecting subtle lateral movements in a complex network.

Algorithmic Bias – Related terms: machine learning, AI ethics. Systematic error introduced by training data that leads to unfair outcomes. Example: An AI triage tool under-prioritizes patients of certain ethnicities. Challenge: Auditing models for bias before deployment in clinical settings.

Anti-Malware – Related terms: virus scanner, endpoint protection. Software designed to detect, prevent, and remove malicious code. Example: Deploying anti-malware on all nursing workstations to block ransomware. Challenge: Keeping signatures up-to-date without impacting device performance.

Application Security – Related terms: secure coding, vulnerability scanning. Practices that protect software applications from threats throughout their lifecycle. Example: Conducting code reviews for a mobile health app before release. Challenge: Integrating security testing into fast-paced development cycles.

Audit Trail – Related terms: log file, forensic analysis. Chronological record of system activities that provides evidence of who did what and when. Example: An audit trail shows a nurse accessed a patient record after hours. Challenge: Retaining logs long enough for investigations while complying with storage regulations.

Authentication – Related terms: multi-factor authentication (MFA), password policy. Process of verifying the identity of a user or device. Example: Using a smart card plus PIN to log into the EHR. Challenge: User resistance to extra steps and managing credential lifecycles.

Authorization – Related terms: access control, permissions. Granting an authenticated entity the right to perform specific actions. Example: A nurse authorized to view vitals but not to edit medication orders. Challenge: Keeping permission sets synchronized with role changes.

Backup and Recovery – Related terms: disaster recovery, data redundancy. Procedures for copying data to a secure location and restoring it after loss. Example: Nightly backups of imaging archives stored off-site. Challenge: Ensuring backups are not also infected by malware.

Biometric Authentication – Related terms: fingerprint, facial recognition. Use of unique physiological traits to verify identity. Example: A fingerprint scanner unlocks a medication cart. Challenge: False-reject rates and

privacy concerns about biometric data storage.

Blockchain – Related terms: distributed ledger, immutable record. Decentralized technology that records transactions in a tamper-evident chain. Example: Using blockchain to verify consent forms. Challenge: High computational cost and limited scalability for large health datasets.

Brute-Force Attack – Related terms: password cracking, credential stuffing. Automated attempts to guess passwords by trying many combinations. Example: Attackers try millions of password combos against a hospital portal. Challenge: Implementing account lockout policies without disrupting legitimate users.

Business Associate Agreement (BAA) – Related terms: HIPAA, vendor contract. Legal contract that outlines responsibilities of a third-party handling protected health information (PHI). Example: A cloud service provider signs a BAA before storing EMR data. Challenge: Ensuring all subcontractors are covered by the same agreement.

CAPTCHA – Related terms: bot mitigation, human verification. Challenge-response test to determine whether a user is human. Example: A login page requires a CAPTCHA after multiple failed attempts. Challenge: Accessibility for users with visual impairments.

Certificate Authority (CA) – Related terms: PKI, digital certificate. Trusted entity that issues and manages public key certificates. Example: The hospital's CA signs certificates for internal web servers. Challenge: Protecting the CA's private key from compromise.

Change Management – Related terms: ITIL, configuration control. Structured approach for introducing updates to systems while minimizing risk. Example: Scheduling a patch rollout for all clinical workstations during low-volume periods. Challenge: Coordinating with clinical staff to avoid service interruptions.

Cloud Security – Related terms: SaaS, IaaS, shared responsibility model. Measures to protect data, applications, and services hosted in cloud environments. Example: Encrypting patient data before uploading to a cloud-based analytics platform. Challenge: Understanding the division of security duties between provider and healthcare organization.

Compromised Credential – Related terms: password leak, credential reuse. User login information that has been exposed and may be used by attackers. Example: A nurse's password appears in a public breach database. Challenge: Promptly resetting passwords and educating staff on unique credentials.

Confidentiality – Related terms: privacy, data protection. Principle that information should be accessible only to authorized individuals. Example: Encrypting PHI during transmission over the hospital network. Challenge: Balancing confidentiality with the need for rapid information sharing in emergencies.

Control Plane – Related terms: network management, SDN. Layer that configures and manages data-plane traffic flows. Example: An SDN controller sets firewall rules for a telehealth subnet. Challenge: Securing the control plane against unauthorized configuration changes.

Cyber Hygiene – Related terms: security best practices, user awareness. Routine practices that maintain system health and reduce vulnerability. Example: Regularly updating software on bedside monitors.

Challenge: Sustaining consistent habits across all staff levels.

Data Loss Prevention (DLP) – Related terms: content inspection, exfiltration control. Technologies that monitor and protect data from unauthorized transfer. Example: DLP blocks copying of PHI to an external USB drive. Challenge: Reducing false positives that impede legitimate clinical workflows.

Data Minimization – Related terms: least data principle, GDPR. Collecting only the data necessary for a specific purpose. Example: Storing only essential demographic fields for a clinical trial. Challenge: Determining the minimal dataset without compromising care quality.

De-Identification – Related terms: anonymization, HIPAA Safe Harbor. Process of removing personal identifiers from data sets. Example: Removing name, SSN, and dates from a research database. Challenge: Re-identification risk when data are combined with external sources.

Defense-in-Depth – Related terms: layered security, security architecture. Strategy of employing multiple defensive measures across layers. Example: Firewalls, intrusion detection, endpoint protection, and employee training combined to protect a radiology department. Challenge: Coordinating controls to avoid gaps and redundancies.

Denial-of-Service (DoS) – Related terms: availability, traffic flooding. Attack that overwhelms a system, rendering it unavailable to legitimate users. Example: A DoS targets the hospital's patient portal, preventing online appointments. Challenge: Maintaining service continuity while filtering malicious traffic.

Digital Forensics – Related terms: evidence collection, incident response. Scientific methods for preserving, analyzing, and presenting digital evidence. Example: Imaging a compromised server to trace ransomware entry. Challenge: Performing forensic imaging without disrupting critical clinical services.

Encryption – Related terms: AES, TLS, data at rest. Process of converting plaintext into ciphertext to protect confidentiality. Example: Encrypting backup tapes of imaging studies. Challenge: Managing encryption keys securely across multiple facilities.

Endpoint Detection and Response (EDR) – Related terms: host-based IDS, threat hunting. Solutions that monitor endpoints for suspicious activity and enable rapid remediation. Example: EDR alerts when a nursing workstation runs an unauthorized script. Challenge: Tuning alerts to avoid overwhelming security staff.

Enterprise Risk Management (ERM) – Related terms: risk assessment, governance. Systematic approach to identifying, evaluating, and mitigating risks across an organization. Example: Conducting a risk assessment for a new telehealth service. Challenge: Aligning risk appetite with clinical imperatives.

Ethical Hacking – Related terms: penetration testing, red team. Authorized attempts to exploit vulnerabilities to improve security. Example: A certified ethical hacker simulates ransomware on a mock ICU network. Challenge: Ensuring tests do not interfere with patient care.

Exfiltration – Related terms: data theft, outbound traffic monitoring. Unauthorized transfer of data from a system to an external location. Example: Malware sends PHI to a remote command-and-control server. Challenge: Detecting low-volume exfiltration that mimics normal traffic.

Failover – Related terms: redundancy, high availability. Automatic switching to a standby system upon failure of the primary. Example: A redundant PACS server takes over when the primary crashes. Challenge: Testing failover without disrupting ongoing imaging studies.

Federated Identity Management – Related terms: SAML, single sign-on (SSO). System that allows users to access multiple applications using a single set of credentials. Example: Nurses use their hospital credentials to log into a third-party scheduling app. Challenge: Trust relationships between disparate providers.

Firewall – Related terms: packet filtering, next-generation firewall. Network device that enforces security policies by controlling inbound and outbound traffic. Example: A firewall blocks inbound connections to the EMR from the public internet. Challenge: Keeping rule sets current with evolving service needs.

Firmware – Related terms: embedded software, device update. Low-level software that controls hardware functions. Example: Updating the firmware of infusion pumps to patch a known vulnerability. Challenge: Coordinating updates across many devices without causing downtime.

Phishing – Related terms: social engineering, spear phishing. Deceptive communication that tricks recipients into revealing credentials or installing malware. Example: A nurse receives an email appearing to be from IT requesting password reset. Challenge: Training staff to recognize sophisticated, targeted attacks.

Physical Security – Related terms: access badge, CCTV, secure storage. Measures that protect hardware and facilities from physical threats. Example: Locked medication cabinets with biometric access. Challenge: Integrating physical controls with logical access policies.

Privacy Impact Assessment (PIA) – Related terms: risk assessment, data protection. Evaluation of how a project affects individual privacy and how risks are mitigated. Example: Conducting a PIA before launching a patient-facing mobile app. Challenge: Balancing thorough analysis with rapid project timelines.

Privilege Escalation – Related terms: vertical escalation, exploit. Attack where a user gains higher access rights than authorized. Example: Malware leverages a system vulnerability to obtain administrator rights on a nursing workstation. Challenge: Detecting escalation in environments with many privileged accounts.

Public Key Infrastructure (PKI) – Related terms: digital certificates, encryption. Framework for creating, managing, distributing, and revoking digital certificates. Example: PKI issues certificates for secure email between physicians. Challenge: Maintaining certificate lifecycle and revocation lists.

Ransomware – Related terms: crypto-locker, extortion. Malware that encrypts data and demands payment for decryption keys. Example: A ransomware strain encrypts a hospital's radiology archive. Challenge: Restoring from backups while maintaining continuity of care.

Remote Access VPN – Related terms: site-to-site, split tunneling. Encrypted tunnel that allows users to connect to the internal network from outside locations. Example: A traveling nurse uses a VPN to access the EMR from a hotel. Challenge: Preventing VPN misuse and ensuring strong authentication.

Risk Assessment – Related terms: threat modeling, vulnerability analysis. Process of identifying potential threats, evaluating vulnerabilities, and estimating impact. Example: Assessing the risk of IoT infusion pumps

being hijacked. Challenge: Quantifying risk in clinical environments where patient safety is paramount.

Security Information and Event Management (SIEM) – Related terms: log aggregation, correlation engine. Platform that collects, normalizes, and analyzes security events in real time. Example: SIEM correlates failed login attempts with unusual data transfers from a nurse's workstation. Challenge: Managing volume of logs while maintaining meaningful alerts.

Security Operations Center (SOC) – Related terms: incident response, threat monitoring. Centralized team responsible for monitoring, detecting, and responding to security incidents. Example: The hospital SOC investigates a suspected breach of PHI. Challenge: Staffing the SOC with clinicians who understand healthcare workflows.

Segmentation – Related terms: network zoning, VLAN. Dividing a network into separate zones to limit lateral movement. Example: Isolating the medical device network from the corporate LAN. Challenge: Ensuring necessary communication between zones for clinical operations.

Social Engineering – Related terms: phishing, pretexting. Manipulative tactics that exploit human trust to gain unauthorized access. Example: An attacker pretends to be a vendor and convinces a nurse to disclose a password. Challenge: Ongoing education to reinforce skepticism.

Supply Chain Attack – Related terms: third-party risk, software dependency. Compromise of hardware or software components before they reach the target organization. Example: Malicious code inserted into a firmware update for cardiac monitors. Challenge: Vetting suppliers and validating integrity of updates.

Threat Intelligence – Related terms: IOCs, STIX/TAXII. Information about current or emerging threats that can be used to improve defenses. Example: Using threat feeds to block known ransomware C2 domains. Challenge: Filtering noise to focus on actionable intelligence.

Tokenization – Related terms: data masking, PCI DSS. Replacing sensitive data with non-sensitive equivalents (tokens) that have no exploitable value. Example: Tokenizing credit card numbers in billing systems. Challenge: Maintaining token mapping for legitimate retrieval while securing the token vault.

Two-Factor Authentication (2FA) – Related terms: MFA, OTP. Security process requiring two distinct forms of verification. Example: Sending a one-time password to a nurse's mobile device after password entry. Challenge: Managing device loss and ensuring reliable delivery.

Unauthorized Access – Related terms: intrusion, breach. Entry into a system or data set without permission. Example: An external hacker accesses the oncology database. Challenge: Detecting unauthorized access quickly to limit exposure.

Vulnerability Management – Related terms: patch management, CVE. Ongoing process of identifying, prioritizing, and remediating security weaknesses. Example: Applying a critical patch to a legacy imaging server. Challenge: Balancing patch urgency with clinical downtime constraints.

Virtual Private Network (VPN) – Related terms: encryption, tunnel. Secure method for transmitting data over public networks by creating an encrypted tunnel. Example: Telehealth providers use a VPN to connect to the

hospital's EHR. Challenge: Configuring split tunneling safely to avoid data leakage.

Vulnerability Scan – Related terms: automated scanner, Nessus. Automated tool that probes systems for known weaknesses. Example: Weekly scans reveal an outdated SSH version on a lab server. Challenge: Interpreting scan results and prioritizing remediation.

Whitelisting – Related terms: application control, allow list. Technique that permits only approved applications to execute. Example: Only certified medical imaging software is allowed on radiology workstations. Challenge: Keeping the whitelist current as new tools are introduced.

Zero-Trust Architecture – Related terms: microsegmentation, continuous verification. Security model that assumes no implicit trust, verifying every request as if it originates from an open network. Example: Each device, user, and application must authenticate before accessing PHI, even within the internal network. Challenge: Redesigning legacy systems to meet continuous verification requirements.