



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Healthcare Add-on
Release Date	September 2025
Next Review	August 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.1

1. What is the Healthcare Add-on

Healthcare is a high-risk, highly regulated sector that faces unique cybersecurity challenges. Hospitals and clinics are prime targets for cyberattacks – incidents can delay critical procedures and disrupt vital services, with the health sector reporting more attacks than any other critical sector. At the same time, healthcare organizations handle very sensitive personal data (patient health information) and must comply with strict laws on privacy and safety (e.g. GDPR for data protection, EU medical device and pharmaceutical regulations). The ShieldNet Healthcare Add-on extends the core ShieldNet Cybersecurity Standard to address these sector-specific needs. ShieldNet’s core provides 48 plain-language controls as a baseline for all SMEs and NGOs, and it was designed to be modular for different industries. This Healthcare Add-on builds on that foundation with additional controls tailored to healthcare providers, hospitals, medical device makers, labs, pharmaceutical companies, and healthcare supply chain entities. The add-on retains ShieldNet’s practical, actionable style – each control is concise (“must-do” statements) and geared for small to medium organizations. By augmenting the core standard with healthcare-specific safeguards, organizations can better protect patient safety, ensure continuity of care, and meet healthcare regulations. This need is underscored by new EU initiatives that explicitly bring more healthcare entities under cybersecurity laws (e.g. the NIS2 Directive now covers medical device manufacturers, pharmaceutical producers, and R&D labs as critical entities). In short, the Healthcare Add-on provides a focused security playbook for the healthcare sector’s unique risks and obligations, in harmony with ShieldNet’s mission to keep security manageable for smaller teams.

2. How to use the Healthcare Add-on

The Healthcare Add-on is meant to be adopted alongside the core ShieldNet controls, not as a standalone list. Healthcare organizations should first implement all relevant core controls (the baseline applicable to all sectors) and then augment them with the sector-specific controls from this add-on. Each healthcare entity should identify which category (or categories) below fit its profile – e.g. a small community clinic would refer to Healthcare Providers, a large general hospital to Hospitals, a biotech startup to R&D Organizations, etc. If an organization spans multiple categories (for instance, a hospital with a research wing, or a pharmaceutical company with its own labs and distribution), it should combine the applicable controls from each relevant section into its security program. The add-on's controls are grouped into the same five Action Zones (Know & Plan, Shield & Build, Watch & Patch, React & Recover, Learn & Lift) used in the core ShieldNet Standard, making it easy to slot these additional requirements into the existing framework.

ShieldNet follows a risk-based approach based on organization size and sector sensitivity. Healthcare is considered a high-sensitivity sector – patient safety and data confidentiality are critical. Thus, for any small or medium healthcare organization, these add-on controls should be treated as mandatory enhancements to the core controls (not optional). A micro-scale healthcare entity (e.g. a solo doctor's office) should still implement as many add-on controls as feasible based on risk – at minimum those addressing legal obligations (like patient data protection) – even if some advanced measures might be scaled down due to limited capacity. Small and medium healthcare entities (up to ~250 staff) are expected to implement the full set of relevant add-on controls; medium-sized ones should additionally prepare for potential audits or oversight on these sector-specific requirements (since regulators often scrutinize healthcare cybersecurity for larger providers). In practice, this means integrating the add-on controls into policies, procedures, and training: for example, a hospital would update its incident response plan to include healthcare-specific steps from this document, and a medical device SME would incorporate these controls into its product development and quality processes.

3. Action Zones

The controls in each category are organized by the five Action Zones to mirror the security lifecycle. Healthcare organizations should address all five zones for a comprehensive program:

- KNOW & PLAN – understanding assets, risks, and regulations in the healthcare context and planning accordingly;
- SHIELD & BUILD – implementing protective measures and secure architectures tailored to healthcare operations;
- WATCH & PATCH – monitoring for issues and keeping systems up-to-date given healthcare’s threat landscape;
- REACT & RECOVER – responding to incidents in a way that prioritizes patient safety and service continuity;
- LEARN & LIFT – learning from incidents/changes to continuously improve and adapt to new healthcare cybersecurity challenges.

Each control below is written in plain language and directly applicable. We reference EU regulations and standards (like MDR, IVDR, GMP Annex 11/15, GDPR) where relevant to show alignment – adhering to these controls will help meet those legal requirements. Use this add-on as a checklist or extension of your core ShieldNet implementation: integrate the controls into your risk assessments, update your security policy to cover these items, and assign responsibility (Info-Sec Coordinator, IT staff, clinical staff, etc.) for each. By following both the core and healthcare-specific controls, even small healthcare organizations can achieve a level of security and compliance proportionate to the sensitivity of their work, while keeping the approach practical and scaled to their size.



3.1. COMMON CONTROLS

The Common Controls are the baseline cybersecurity requirements for all healthcare organizations in the ShieldNet program (SMEs, clinics, hospitals, labs, medtech, pharma, and supply-chain actors). They extend the Core Standard with patient-safety and data-protection specifics and are organized under the five Action Zones. Each control is proportionate for small teams, written in plain English, and directly traceable to EU healthcare sources (e.g., GDPR, MDR/IVDR, Annex 11/15, cross-border eHealth). Implement these first, keep the evidence lightweight but current (using the Annex A templates), and you'll have a defensible, audit-ready baseline that protects patients, safeguards data, and supports uninterrupted care.

3.1.1. *KNOW & PLAN*

[KP-H1] Classify Patient Data

Control text: Classify patient health information and other sensitive data into a few clear categories so everyone knows what needs stronger protection. For each category, define simple rules for access, sharing, storage, retention, and secure disposal, and make them easy for staff to follow. Review the rules at least once a year and after major changes.

Why: Unclassified or unprotected sensitive data can be easily exposed, compromising patient privacy and trust.

Evidence examples: Data classification policy, access control lists, encryption implementation records, staff training materials on data handling.

Legal anchors: GDPR Art. 5(1)(f), GDPR Art. 25(1), GDPR Art. 32(1), MDR Annex XV.4.

[KP-H2] Integrate Cyber Risk Management

Control text: Include cybersecurity risks in your regular risk management process and treat them as business and patient safety risks. Record the key risks, decide how you will reduce them, and track actions until they are closed. Review the risks regularly and after major changes to systems, suppliers, or services.

Why: Unaddressed cyber risks can disrupt healthcare operations or expose sensitive information, directly impacting patient safety.

Evidence examples: Risk assessment reports with cybersecurity elements, enterprise risk register entries for cyber threats, meeting minutes on security risk decisions.

Legal anchors: NIS2 Art. 21(2)(a), EudraLex Vol. 4 Annex 11 §1, MDR Annex I 17.2.

[KP-H3] Assign a Privacy Lead

Control text: Assign a privacy lead who is responsible for data protection and security topics linked to patient information. Define their responsibilities, including handling data subject requests, overseeing breaches, and coordinating with IT and clinical teams. Give them the authority, time, and a clear path to escalate issues to leadership.

Why: Clear privacy leadership reduces legal risk, speeds breach response, and embeds “privacy by design” into everyday work; without it, obligations are missed.

Evidence examples: Appointment letter/contract, role description with independence statement, leadership reporting line, DPIA/advice log, training/awareness plan.

Legal anchors: GDPR Art. 37(1)–(3), GDPR Art. 38, GDPR Art. 39.

3.1.2. SHIELD & BUILD

[SB-H1] Control Access to Health Systems

Control text: Limit access to electronic health records and other clinical systems to people who need it for their role. Use role based access, strong authentication, and approvals for privileged access. Review access regularly and remove it quickly when roles change or staff leave.

Why: Poor access controls enable unauthorized viewing or tampering of patient data and vital systems.

Evidence examples: Access control policy, list of user accounts/roles, multi-factor authentication logs, user access review reports

Legal anchors: EudraLex Vol. 4 Annex 11 §12.1, GDPR Art. 32(1)(b).

[SB-H2] Segment Clinical and Device Networks

Control text: Separate networks for medical devices and key clinical systems from office and guest networks to reduce the spread of attacks. Allow only the connections that are needed for care and block the rest with simple firewall rules. Document the intended connections and review them after changes.

Why: Unsegmented networks allow malware or hackers to spread from one system to another, endangering patient services.

Evidence examples: Network diagrams with VLAN segmentation, firewall configuration rules, network penetration test reports, inventory of networked medical devices.

Legal anchors: NIS2 Art. 21(2)(e), MDR Annex I 16.4.

[SB-H3] Harden Systems and Devices

Control text: Harden servers, endpoints, and medical devices by applying secure settings and removing or disabling what you do not need. Change default passwords, restrict remote access, and keep unnecessary services turned off. Document a short baseline configuration and check it periodically.

Why: Systems left with default settings or unnecessary services are easily exploited, jeopardizing patient data or system functionality.

Evidence examples: System hardening checklists, device configuration change logs, records of default credential changes, security configuration compliance scans.

Legal anchors: NIS2 Art. 21(2)(e), EudraLex Vol. 4 Annex 11 §10

[SB-H4] Encrypt Sensitive Health Data

Control text: Encrypt sensitive health data when it is stored and when it is sent between systems and to external parties. Use managed keys and restrict who can access decryption, especially for backups and exports. Make sure portable media and file transfers are encrypted and controlled.

Why: Encryption reduces harm if data is lost or stolen.

Evidence examples: TLS configuration evidence, database or disk encryption settings, encrypted backup logs, key management procedure.

Legal anchors: NIS2 Art. 21(2)(h), GDPR Art. 32(1)(a).

3.1.3. WATCH & PATCH

[WP-H1] Monitor Systems and Devices

Control text: Monitor critical systems and medical devices for security events, outages, and unusual behavior. Collect key logs and set simple alerts for high risk events such as failed logins, admin activity, and blocked malware. Ensure someone reviews alerts and takes action every day.

Why: Without active monitoring, cyber-attacks or system failures can go undetected until they cause significant damage or downtime.

Evidence examples: Monitoring dashboard or SIEM alerts, IDS logs, alert handling procedure, sample incident tickets.

Legal anchors: NIS2 Art. 21(2)(b), EudraLex Vol. 4 Annex 11 §11.

[WP-H2] Patch and Fix Vulnerabilities

Control text: Patch systems and fix vulnerabilities on a defined schedule so known issues are closed quickly. Prioritize critical and exposed systems, including remote access services and clinical applications. When patching is not possible, use temporary mitigations and track the plan to fix it.

Why: Unpatched systems can be exploited by attackers, leading to data breaches or device malfunctions.

Evidence examples: Vulnerability scan reports, patch management logs, change management tickets for security updates, device firmware version listings.

Legal anchors: NIS2 Art. 21(2)(e), EudraLex Vol. 4 Annex 11 §11.

[WP-H3] Keep Audit Logs and Review Them

Control text: Enable audit logs for key systems such as identity services, EHR access, and administrative actions. Protect logs from tampering and make sure they are available to support investigations and compliance. Retain logs for an agreed period and review important events regularly.

Why: If audit logs are not kept and reviewed, unauthorized access or alterations may go unnoticed, undermining data integrity and privacy.

Evidence examples: System audit trail configurations, access log files, periodic log review reports, documented follow-up on suspicious log events.

Legal anchors: EudraLex Vol. 4 Annex 11 §9, GDPR Art. 32(1)(d).

3.1.4. REACT & RECOVER

[RR-H1] Incident Response Planning

Control text: Prepare an incident response plan for cyber incidents that could affect patient data or continuity of care. Define roles, contact details, decision steps, and when to involve legal, regulators, and suppliers. Test the plan with a simple exercise and update it after lessons learned.

Why: A chaotic or delayed response to incidents can worsen damage, prolong downtime, and increase harm to patients and operations.

Evidence examples: Approved incident response plan document, incident playbooks/runbooks, incident response team roster, results of incident response drills.

Legal anchors: NIS2 Art. 21(2)(b), EudraLex Vol. 4 Annex 11 §13, GDPR Art. 33(5).

[RR-H2] Back Up and Test Recovery

Control text: Back up critical clinical systems and data such as EHR, imaging, and key configurations on a regular schedule. Store backups securely and separately, and protect them from deletion or encryption. Test restores to prove you can recover within your required time.

Why: Unrecoverable data loss (e.g. from ransomware or hardware failure) can severely disrupt patient care or research activities.

Evidence examples: Backup schedule and logs, off-site backup storage records, disaster recovery test reports demonstrating successful data restore, verification of backup data integrity.

Legal anchors: NIS2 Art. 21(2)(c), EudraLex Vol. 4 Annex 11 §7.2, GDPR Art. 32(1)(c).

[RR-H3] Plan Continuity of Care

Control text: Plan how you will continue clinical operations if key systems are unavailable due to an incident or outage. Define manual workarounds and priority services, and make sure staff know where to find the procedures. Practice the plan and adjust it based on results.

Why: IT failures without fallback processes can halt patient care or vital operations, putting lives and business at risk.

Evidence examples: Business Continuity Plan (BCP) for clinical operations, emergency downtime procedure manuals, training records for staff on manual procedures, generator/backup system test logs.

Legal anchors: NIS2 Art. 21(2)(c), Directive 2011/24/EU Art. 14(2)(a).

3.1.5. LEARN & LIFT

[LL-H1] Train Staff on Cyber Hygiene

Control text: Train staff on basic cyber hygiene using healthcare examples such as phishing, password reuse, and handling patient data. Provide training during onboarding and refresh it regularly, especially for clinical and frontline roles. Track completion and address gaps with targeted reminders.

Why: Untrained employees can inadvertently cause breaches (for example, by falling for scams or mishandling sensitive information).

Evidence examples: Cybersecurity training curriculum and materials, staff training attendance logs, phishing simulation results, employee cybersecurity quiz scores.

Legal anchors: NIS2 Art. 21(2)(g), EudraLex Vol. 4 Annex 11 §2.

[LL-H2] Security Audits and Assessments

Control text: Review and test your controls to confirm they work in daily operations and during high pressure situations. Use simple checks such as access reviews, backup restore tests, and phishing simulations, then record findings. Fix issues, assign owners, and report progress to management.

Why: Regular checks find gaps before attackers do.

Evidence examples: Internal audit reports, third-party penetration test reports, management action plans for audit findings, updated procedures addressing identified gaps.

Legal anchors: NIS2 Art. 21(2)(f), EudraLex Vol. 4 Annex 11 §11.

[LL-H3] Incident Lessons Learned

Control text: Assess cybersecurity risks that could impact patient safety, especially where devices and clinical workflows depend on IT. Identify the most likely scenarios, decide how you will reduce harm, and document what is acceptable risk. Review the assessment after major changes, new devices, or serious incidents.

Why: If the organization does not learn from incidents, the same vulnerabilities will be exploited again, causing repeat harm.

Evidence examples: Post-incident review reports, incident “lessons learned” meeting minutes, revised security policies or configurations after incidents, updated risk assessment reflecting the incident.

Legal anchors: EudraLex Vol. 4 Annex 11 §13, NIS2 Art. 21(2)(b).

3.2. CATEGORY SPECIFIC CONTROLS

The Category-Specific Controls add focused requirements for particular healthcare contexts where risks and workflows differ (Hospitals; Healthcare Providers; Diagnostics; Medical Device Manufacturers; MedTech; Pharmaceutical & R&D; Supply Chain). Start with the Common Controls, then layer only the categories that match your scope. Each add-on narrows the “how” for your environment—clinical networks and downtime care in hospitals, validated LIMS and PACS in diagnostics, secure-by-design and SBOM for device makers, GxP data integrity for pharma/R&D, and traceability for supply chains—while preserving the same format, evidence style, and legal mapping used throughout the standard.

3.2.1. Hospitals

[KP-H4] Assess Patient Safety Cyber Risks

Control text: Assess cybersecurity risks that could impact patient safety, especially where devices and clinical workflows depend on IT. Identify the most likely scenarios, decide how you will reduce harm, and document what is acceptable risk. Review the assessment after major changes, new devices, or serious incidents.

Why: Untrained employees can inadvertently cause breaches (for example, by falling for scams or mishandling sensitive information).

Evidence examples: Cybersecurity training curriculum and materials, staff training attendance logs, phishing simulation results, employee cybersecurity quiz scores.

Legal anchors: NIS2 Art. 21(2)(a), MDR Annex I 17.2.

[SB-H5] Isolate Life Critical Devices

Control text: Isolate life critical devices and their supporting systems to reduce exposure to office networks and the internet. Limit who can access them, restrict remote connections, and use approved maintenance paths with strong authentication. Monitor these segments closely and coordinate changes with clinical owners and vendors.

Why: Critical devices can malfunction or endanger patients if infected; network isolation prevents malware from spreading from office IT into treatment equipment.

Evidence examples: Network diagrams showing separate VLANs for medical devices, firewall rules restricting traffic to medical network, test results confirming isolation of device network.

Legal anchors: MDR Annex I 18.8, NIS2 Art. 21(2)(e).

[RR-H4] Clinical Downtime Procedures

Control text: Prepare clinical downtime procedures for EHR, imaging, labs, and other critical services so care can continue safely. Include clear steps, paper forms, contact lists, and how to record and later reconcile data. Train staff on the procedures and practice them periodically.

Why: If digital systems fail with no fallback process, clinicians may be unable to access records or equipment, leading to dangerous delays or errors in treatment.

Evidence examples: Emergency downtime protocols (paper forms, offline data access methods), staff training logs for executing manual procedures, drills demonstrating patient care during IT outages.

Legal anchors: NIS2 Art. 21(2)(c), Directive 2011/24/EU Art. 14(2)(a).

3.2.2. Healthcare Providers

[SB-H6] Secure Patient Data Exchange

Control text: Secure patient data exchange between systems and partners, including interfaces and integrations used for care. Use strong authentication, encryption, and least privilege for service accounts and APIs. Validate data flows, monitor for errors and misuse, and review partner access regularly.

Why: Insecure data exchange (for example, sending medical files over unencrypted email) can leak sensitive patient information or hinder care if data is lost or altered.

Evidence examples: Use of approved health information exchange platforms, encryption certificates for email or data transfer, policy for cross-border data sharing, audit logs of data exchanges.

Legal anchors: GDPR Art. 32(1), Directive 2011/24/EU Art. 14(2)(a).

[SB-H7] Secure Telemedicine Practices

Control text: : Secure telemedicine services so appointments and patient data are protected from interception and unauthorized access. Use strong authentication for staff, protect meeting links, and apply settings that prevent unwanted recording or sharing. Store recordings and transcripts securely and limit access to those who need it.

Why: Telemedicine involves sensitive conversations that must stay confidential.

Evidence examples: Telemedicine usage policy, signed patient consent forms for telehealth, records of using an accredited telehealth platform with end-to-end encryption, IT assessment of telemedicine tools.

Legal anchors: MDR Annex XV.4.5, GDPR Art. 5(1)(f), GDPR Art. 32(1), Directive 2011/24/EU Art. 14(2)(a).

[RR-H5] Keep Critical Patient Info Available

Control text: Ensure critical patient information stays available during outages so clinicians can make safe decisions. Keep an offline or read only copy of key datasets such as allergies, medications, and emergency contacts, and update it on a defined schedule. Protect this access and test that staff can use it when needed.

Why: If doctors cannot retrieve key patient data during a system downtime, it can lead to treatment errors or dangerous delays in care.

Evidence examples: Printed or downloaded patient summary sheets for emergency use, procedure for accessing backup medical records, testing records of retrieving patient info during EHR outages.

Legal anchors: NIS2 Art. 21(2)(c), Directive 2011/24/EU Art. 14(2)(a).

3.2.3. Diagnostics Labs

[KP-H5] Validate Lab Systems

Control text: Validate laboratory systems and connected instruments so results are reliable and security controls are in place. Document key requirements such as access control, audit trails, and data integrity checks, and confirm they work as intended. Revalidate after significant changes, updates, or new integrations.

Why: Unvalidated lab software might produce incorrect test results or fail without detection, risking misdiagnosis or delayed treatment for patients.

Evidence examples: Validation plan and report for each lab system, IQ/OQ/PQ* records for lab equipment software, documented test cases verifying result accuracy and system reliability.

Legal anchors: EudraLex Vol. 4 Annex 11 Principle, EudraLex Vol. 4 Annex 15.

[SB-H8] Restrict Access to Lab Data

Control text: Restrict access to laboratory data and systems so only authorized users can view or change results. Use roles for tasks such as entry, review, and approval, and limit privileged access to a small group. Review access regularly and remove it quickly when roles change.

Why: Unauthorized access to lab data or systems can lead to data breaches or result manipulation, undermining trust in diagnostics.

Evidence examples: User and role list, access approval process, access review record, lab system access logs.

Legal anchors: EudraLex Vol. 4 Annex 11 §12.1, GDPR Art. 32(1)(b).

[WP-H4] Use Lab Audit Trails

Control text: Enable audit trails in lab systems so you can track who created, changed, and approved results. Review audit logs for unusual activity such as repeated edits, access outside normal hours, or changes after approval. Retain logs long enough to support investigations and regulatory needs.

Why: Audit trails deter tampering and help explain corrections.

Evidence examples: Audit trail settings, audit review log, change records with justification, QA review notes.

Legal anchors: EudraLex Vol. 4 Annex 11 §9.

3.2.4. MedTech

[SB-H9] Secure Development Lifecycle

Control text: Use a secure development process for clinical applications, integrations, and scripts that you build or customize. Include code review, dependency management, and basic security testing before release. Keep release notes and make sure fixes for security issues are prioritized.

Why: Fixing issues early is cheaper than patching in production.

Evidence examples: Secure development policy, threat model document, code review checklist, security test report.

Legal anchors: NIS2 Art. 21(2)(e), Regulation (EU) 2017/745 Annex I 17.2, Regulation (EU) 2017/746 Annex I 16.2.

[SB-H10] Define Customer Security Requirements

Control text: Define customer security requirements for how your service or product must be deployed and operated safely. Provide clear configuration guidance, required access settings, and minimum logging and patching expectations. Review requirements over time and update them when threats or features change.

Why: A secure product can still be unsafe if installed badly.

Evidence examples: Implementation guide, security configuration checklist, customer sign off, support knowledge base.

Legal anchors: Regulation (EU) 2017/746 Annex I 16.4, Regulation (EU) 2017/745 Annex I 17.2.

3.2.5. Medical Device Manufacturers

[KP-H6] Manage Cyber Risks in Design

Control text: Manage cyber risks during design by identifying what could go wrong and what needs protection. Use a simple threat review for key features, data flows, and integrations, then choose controls that reduce the risk. Document decisions and get sign off before going live.

Why: Cyber weaknesses can become patient safety risks.

Evidence examples: Risk management file with cyber risks, design review minutes, security requirements list, documented mitigations.

Legal anchors: MDR Annex I 17.2.

[SB-H11] Verify and Validate Device Software

Control text: Verify and validate device software before release and after updates so you can trust what is running. Use secure build and update processes, including code signing and checks that prevent unauthorized packages. Record test results and approvals for each release.

Why: Testing finds weaknesses before patients depend on the device.

Evidence examples: Software verification and validation report, security test results, validation protocol, defect and fix log.

Legal anchors: MDR Annex II 6.3.

[SB-H12] Protect Device Software and Data

Control text: Protect device software and stored data from unauthorized changes and tampering. Use controls such as secure boot, restricted admin access, and protection of configuration and logs. Monitor for integrity issues and respond quickly if changes are detected.

Why: Built in controls help keep devices safe in real world networks.

Evidence examples: Security architecture diagram, secure boot or code signing evidence, encryption and key documentation, test results.

Legal anchors: MDR Annex I 18.8.

[LL-H4] Provide Security Instructions to Users

Control text: Provide clear security instructions to users of your product or service so they can use it safely. Explain how to manage accounts, enable strong authentication, apply updates, and report incidents. Keep guidance easy to find and update it when the product changes.

Why: Users need practical steps to keep devices secure over time.

Evidence examples: Instructions for use security section, update guide, vulnerability reporting contact, customer security bulletins.

Legal anchors: MDR Annex I 23.4, MDR Annex I 16.4.

3.2.6. Pharmaceutical and R&D Organizations

[KP-H7] GxP System Qualification & Validation

Control text: Validate GxP systems that support regulated processes so required controls are implemented and working. Confirm access control, audit trails, data integrity, and backup and recovery meet your requirements. Revalidate after significant changes and keep evidence for audits.

Why: Validated systems support product quality and reliable data.

Evidence examples: Validation master plan, qualification protocols and reports, risk assessment for validation scope, validated systems inventory.

Legal anchors: EudraLex Vol. 4 Annex 11 Principle, EudraLex Vol. 4 Annex 15.

[SB-H13] Protect Data Integrity

Control text: Protect data integrity for clinical and regulated records so changes are controlled and traceable. Use approvals, versioning, and technical checks that prevent silent changes and support accurate audit trails. Limit who can change critical records and review exceptions regularly.

Why: Wrong or altered data can lead to unsafe products and invalid studies.

Evidence examples: SOP for second person checks, dual sign batch record example, audit trail review log, QA data integrity review.

Legal anchors: EudraLex Vol. 4 Annex 11 §6, EudraLex Vol. 4 Annex 11 §9.

[WP-H5] Control Changes to GxP Systems

Control text: Control changes to GxP systems using a formal change process that reduces risk and keeps evidence. Assess impact, test the change, obtain approvals, and record what was changed and why. Track emergency changes and review them after the fact.

Why: Uncontrolled changes or lack of regular review can introduce errors or security gaps, invalidating the system's qualified state and breaching compliance.

Evidence examples: Change request forms and approvals for system updates, change log with impact assessments, periodic IT system review reports, re-validation or qualification test results after significant changes.

Legal anchors: EudraLex Vol. 4 Annex 11 §10, EudraLex Vol. 4 Annex 11 §11.

3.2.7. Healthcare Supply Chain Actors

[KP-H8] Supplier Cybersecurity Assurance

Control text: Set supplier security requirements for vendors that handle patient data or provide systems that affect care. Include expectations for access control, incident notification, patching, and secure support, and make them part of contracts. Check suppliers before onboarding and reassess them periodically.

Why: A supplier incident can disrupt your services and expose sensitive data.

Evidence examples: Contract security clauses, supplier questionnaire, supplier audit report, corrective action plan.

Legal anchors: NIS2 Art. 21(2)(d), GDPR Art. 28(1) and (3), EudraLex Vol. 4 Annex 11 §3.1 and §3.2.

[SB-H14] Secure Product Tracking Systems

Control text: Secure product tracking systems for devices, lots, and patient linkage so records stay accurate and available. Use access control, audit logs, and backups to protect against unauthorized changes or deletions. Protect interfaces and integrations, and review access regularly.

Why: Tampered tracking data can hide counterfeit or unsafe products.

Evidence examples: Access control and logging for tracking system, integrity checks, anomaly handling record, secure API settings.

Legal anchors: MDR Art. 27, Directive 2011/62/EU, Delegated Regulation (EU) 2016/161.