ManageEngine

A quick guide to NEN 7510

NEN 7510-1:2024, issued by the Royal Netherlands Standardization Institute (NEN), is the Dutch standard for information security in healthcare. It sets the requirements for an information security management system (ISMS) that safeguards the availability, integrity, and confidentiality of personal health information.

Sl.no	Requirement area	Articles	Controls required
1	ISMS governance and risk	Clauses 4–6	• Define the ISMS scope and context • Run risk assessments and treatments and assign risk owners • Maintain a Statement of Applicability • Set security objectives and review the system
2	Identity and access governance	A.5.15–5.18 and A.8.2–8.3	• Enforce role-based access to health data • Manage the identity life cycle and external accounts • Review and recertify access rights • Restrict privileged access and separate conflicting duties
3	Secure authentication	A.5.17 and A.8.5	• Require two-factor authentication for PHI systems • Deploy adaptive MFA • Enforce a password complexity policy • Notify users about password expirations
4	Data classification and protection	A.5.9, A.5.12–5.14, and A.5.34	• Classify PHI as confidential and label all data by sensitivity • Inventory information assets and flows • Prevent data leakage and restrict sensitive data access • Protect personal data and privacy
5	Logging, monitoring, and threat detection	A.5.7, A.8.7–8.9, and A.8.15–8.16	• Centralize and retain logs • Monitor for anomalous activity and detect malware • Track configuration changes • Collect threat intelligence and assess vulnerabilities
6	Incident management and reporting	A.5.24–5.28, A.5.43, and A.6.8	• Plan incident response roles and enable staff reporting • Triage and classify events • Respond to incidents via documented procedures • Preserve forensic evidence and report incidents externally
7	Backups, recovery, and continuity	A.5.29–5.30 and A.8.13	• Maintain scheduled backups • Encrypt health data backups • Test point-in-time recovery procedures • Plan ICT continuity readiness
8	Records, media, supplier, and cloud security	A.5.19, A.5.23, A.5.33, A.7.10, and A.8.35	• Protect records and encrypt PHI on removable media • Assess external party access • Secure cloud service usage and filter out malicious content • Apply Zero Trust principles

Source: www.nen.nl/en/nen-7510-1-2024-nl-331311

NEN 7510 and ManageEngine

ManageEngine offers solutions that help healthcare organizations govern access, protect health data, and detect and respond to threats. The capabilities of AD360 (ManageEngine's IAM solution) and Log360 (its SIEM solution) map directly to the technical controls in Annex A of NEN 7510-1. Together, they enable organizations to implement the controls required under NEN 7510.

How can ManageEngine help you implement NEN 7510?

MFA

Enforce adaptive MFA and two-factor authentication on systems that process personal health information.

Helps with A.8.5

Role-based access governance

Govern access to health data based on users' roles with granular delegation and periodic certification.

Helps with A.5.15 and A.8.3

Identity life cycle management

Automate provisioning and deprovisioning so access always reflects current roles.

Helps with A.5.16 and A.5.18

Audit trails and log retention

Centralize, protect, and retain tamper-evident logs for evidence collection and review.

Helps with A.5.28 and A.8.15

Monitoring and anomaly detection

Detect anomalous activity in real time with correlation and behavior analytics across the estate.

Helps with A.8.16

Data classification and DLP

Classify PHI as confidential and block leakage via USB, email, and print media.

Helps with A.5.12 and A.5.14

Incident response and reporting

Run automated playbooks and generate reports for mandatory external incident reporting.

Helps with A.5.26 and A.5.43

Backups and recovery

Maintain AES-256-encrypted backups with point-in-time, granular recovery.

Helps with A.5.30 and A.8.13

Compliance reporting and threat intelligence

Generate audit-ready reports and correlate logs with threat feeds mapped to MITRE ATT&CK®.

Helps with A.5.7 and A.5.43

For more information, contact sales@manageengine.com