Kiteworks

COMPLIANCE BRIEF

FOR DUTCH HEALTHCARE ORGANIZATIONS

Zivver and Kiteworks Are Certified for NEN 7510-1:2024 — Medical Informatics — Information Security in Healthcare — Part 1: Management System

From Zero-Trust Architecture to Real-Time SIEM Feeds: a Technical Path Through Dutch Healthcare's Personal Health Information Obligations

NEN 7510-1:2024 | Netherlands Healthcare | Zivver + Kiteworks

Solution Highlights

- Strong Double Encryption
- Data Policy Engine with ABAC and RBAC
- SafeEDIT
- SafeVIEW
- Comprehensive audit logs with SIEM feeds
- eDiscovery access controls

NEN 7510-1:2024, titled "Medical Informatics — Information Security in Healthcare — Part 1: Management System," is a Dutch national standard published by NEN in 2024, establishing an information security management system for healthcare. It applies to healthcare providers (zorgaanbieders), healthcare institutions (zorginstellingen), and processors of personal health information — hospitals, long-term care facilities, mental health organizations, solo-practicing clinicians, and health information system suppliers — regardless of size, anywhere in the Netherlands.

It sets no monetary fines; compliance flows from requirements across chapters 4 through 10 and Annex A, with enforcement through Dutch healthcare regulation, insurer and government contracts, and Autoriteit Persoonsgegevens oversight, risking sanctions, lost certification, and contractual liability. Zivver, now part of Kiteworks, is named in Certificate NL 3069.1.1: Brand Compliance B.V., a Dutch RvA-accredited body (RvA C 548), verified Zivver Secure Communications Services' ISMS meets NEN 7510-1:2024, valid 6 August 2026 through 31 July 2029. Kiteworks holds this certification and supports organizations pursuing their own compliance.

NEN 7510-1:2024 Zero-Trust Architecture Meets Dutch Healthcare Protection

NEN 7510-1:2024 requires access governance, encrypted health information, physical safeguards, and secure development practices. The Data Policy Engine's ABAC/RBAC controls and least privilege defaults govern data access; SCIM, LDAP/SAML SSO, and external-user management automate identity lifecycle. Multi-factor authentication, required for systems touching personal health information (A.8.5), runs through RADIUS, PIV/CAC, and OTP, alongside RBAC folder roles and expiration settings. Encryption at rest double-encrypts every file; Customer-owned keys and HSM integration keep key custody with the organization; and FIPS 140-3 validated encryption meets the mandate to encrypt removable media and backups (A.7.10, A.8.13). SafeVIEW renders shared files as watermarked, view-only images so personal health information can be reviewed without being copied, downloaded, or forwarded, while SafeEDIT lets authorized users edit those same files inside a virtual desktop streamed to the browser so the file itself never leaves the secure Kiteworks environment; encryption in transit protects both sessions, and admin and end user roles enforce separation of duties. Tiered internal services, zero trust mode, embedded firewalls, AI-based intrusion and anomaly detection, and Fail2Ban form a zero-trust perimeter, with antivirus, threat prevention, file sanitization, high availability, and comprehensive Dev SecOps. ISMS scope, policy, risk acceptance, supplier agreements, and personnel obligations remain the organization's to handle.

Objectives Supported by DPE and Compliance Reports

NEN 7510-1:2024 requires a continually improving information security management system, measurable objectives, periodic risk assessments, and ongoing control monitoring, plus oversight of supplier changes. The Data Policy Engine's ABAC and RBAC controls operationalize the standard's access-governance dimension, while compliance reports covering audit log, insider and outsider threats, GDPR, and HIPAA give measurable evidence of control performance. Comprehensive audit logs with SIEM feeds, normalized into a single stream, provide the evidentiary record risk assessors need. Admin role-based access to tracking data assigns a dedicated compliance role, separating duties, and admin reporting's exportable activity and usage reports address what to monitor and how to validate it. Supplier security monitoring draws on the same consolidated log and compliance reports. Data sovereignty and geofencing satisfy the standard's cloud-governance requirement (A.5.23) by storing and routing data only within a user's assigned country, with residency reporting; Customer-owned keys and Single-tenant private cloud preserve key custody and database isolation regardless of deployment model.

Incident Detection, Evidence Preservation, and Vulnerability Tracking

NEN 7510-1:2024 requires organizations to assess security events, respond to incidents through documented procedures, preserve evidence, give staff a way to report suspected events, monitor networks for anomalies, analyze log files (A.8.15), synchronize clocks, track vulnerabilities and capacity, and maintain threat intelligence. Comprehensive audit logs with SIEM feeds aggregate every security event into a single, unthrottled stream, fed in real time to ArcSight, QRadar, Splunk, and LogRhythm. AI-based intrusion and anomaly detection and topics logged identify suspicious activity, while security analytics through the CISO Dashboard surfaces anomalies before they become breaches. When an event escalates to an incident, log export feeds, the insider threats compliance report, and embedded managed detection and response support the documented response. Trusted audit logs and Legal hold and eDiscovery access controls, limited to Data Leak Investigator Admins, preserve evidence (A.5.28). Secure Data Forms give staff a reporting channel; NTP clock-sync checks and SNMP Health Monitoring with the Node Health API track timestamps, capacity, and vulnerabilities.

Kiteworks addresses NEN 7510-1:2024's personal health information protection obligations through double encryption at rest and in transit, possessionless editing via SafeEDIT, data masking via SafeVIEW, DLP integration, and zero-trust network architecture that enforces mutual authentication across every service boundary. The Data Policy Engine's ABAC and RBAC controls, SCIM-driven identity lifecycle management, and mandatory multi-factor authentication operationalize the standard's role-based access and identity registration requirements for systems processing personal health information. Comprehensive audit logs with SIEM feeds, AI-based Intrusion and Anomaly Detection, legal hold controls, and insider/outsider threats compliance reports give healthcare organizations the continuous monitoring, incident response, and evidence preservation capabilities the standard demands. Kiteworks functions as a unified platform across protection, access governance, and security operations for organizations pursuing conformance with NEN 7510-1:2024.

See How Kiteworks Supports Your NEN 7510-1:2024 Compliance Journey

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.