NEOPHARMA TECHNOLOGIES' COMPREHENSIVE MATURITY FRAMEWORK

EXECUTIVE SUMMARY

Neopharma's Security & Compliance Office (SCO) operates a single, integrated security program that governs our products, people, and platforms. External certifications—SOC 2 Type II, ISO/IEC 27001:2022, HIPAA, and GDPR—are the outcome of that operating model, not the objective. Our controls are defined and monitored year-round (policy, risk, IAM, encryption, secure SDLC, incident response) with continuous compliance automation, internal audits, and management review to keep us audit-ready every day.

Independent validation

SOC 2 Type II for NEOVAULT & myNEO (Aug 2024→Aug 2025) confirms controls relevant to Security, Confidentiality, Availability were suitably designed and operated effectively across the period.

ISO/IEC 27001:2022 certificate current to 26-May-2026; Surveillance-I (Aug 2025) evidences Compliance Management Tool via Sprinto-based continuous monitoring, internal audit, management review, and a risk register with 52 identified risks and mitigation controls.

HIPAA and GDPR compliance continuations valid to 18-Jul-2026.

What this means for clients

Security and privacy are built-in to NEOVAULT & myNEO, supported by encryption in transit and at rest, role-based access control and MFA, continuous monitoring, and tested response. The program lowers adoption risk for enterprise IT/security teams, protects brand and operations for the C-suite, and ensures healthcare customers that PHI and personal data are handled lawfully and securely.

COMPLIANCE SNAPSHOT

Framework	Status	Validity / Period	Scope / Notes
SOC 2 Type II	Active	Aug 2024 → Aug 2025	NEOVAULT & myNEO; criteria: Security, Confidentiality, Availability; independent service auditor's report for the stated period.
ISO/IEC 27001:2022	Certified	to 26-May-2026	ISMS covering NEOVAULT & myNEO; Surveillance-I confirms continuous monitoring, internal audit, management review; 52 identified risks with mitigation controls.
HIPAA	Continuation	to 18-Jul-2026	Continuation letter (2nd surveillance).
GDPR	Continuation	to 18-Jul-2026	Continuation letter (2nd surveillance).

COMPANY & PRODUCT OVERVIEW

NEOPHARMA TECHNOLOGIES LIMITED

Neopharma builds cloud-hosted applications for health testing workflows with uncompromising security and privacy. Our flagship product NEOVAULT® includes the NEOVAULT ERM platform and two mobile applications; the NEOVAULT app and the myNEO app, that handle sensitive medical data, and the SCO embeds security-by-design and privacy-by-design across architecture, operations, and product development.

The healthcare technology landscape demands solutions that balance innovation with security. Against this backdrop, Neopharma has built a comprehensive security framework that not only protects sensitive data but enables healthcare organizations to innovate with confidence.

Our approach reflects deep understanding of healthcare operational requirements. Neopharma addresses these challenges through integrated platform design, proactive security management, and comprehensive compliance coverage that simplifies rather than complicates healthcare operations.

Key Achievement: Neopharma is among the healthcare technology companies maintaining simultaneous compliance across four major frameworks: SOC 2 Type II, ISO 27001:2022, HIPAA, and GDPR.

NEOVAULT: Cloud platform for health testing workflows

NEOVAULT is a cloud-hosted application that centralizes testing programs and reporting, implemented on a VPC-isolated architecture with encryption in transit and at rest, RBAC & MFA, and logging for accountability.

The platform architecture reflects healthcare industry best practices for cloud security. Our implementation includes Virtual Private Cloud (VPC) isolation, multi-layer firewalls, HTTPS/TLS encryption for data in transit, and industry-standard AES-256 encryption for data at rest. These technical safeguards align with AWS Well-Architected Framework security principles and healthcare-specific compliance requirements.

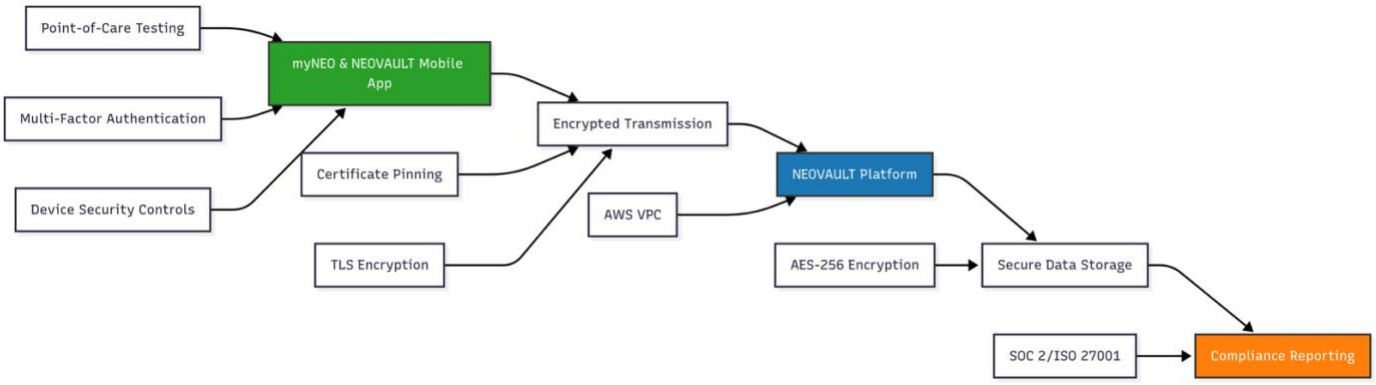
NEOVAULT's integrated approach addresses the complex compliance landscape facing healthcare organizations. Our platform provides healthcare organizations with confidence that their risk management processes meet the highest security standards while enabling operational efficiency.

NEOVAULT and myNEO Apps: Secure point-of-care data capture

The NEOVAULT and myNEO mobile apps augments NEOVAULT with secure collection and encrypted transmission of test data from distributed settings, integrating authentication and mobile safeguards appropriate to handling PHI.

NEOVAULT and myNEO apps address these challenges through comprehensive mobile security architecture including certificate pinning, runtime application self-protection, and secure API communication. Our approach ensures that sensitive health data remains protected throughout the collection, transmission, and storage lifecycle, regardless of testing location or device type.

The application demonstrates our commitment to security-by-design principles. Rather than adding security as an afterthought, NEOVAULT and myNEO apps incorporate encryption, authentication, and access controls as fundamental architecture components.



INTEGRATED SECURITY ARCHITECTURE

Our product ecosystem demonstrates comprehensive security integration across cloud platforms and mobile applications. This architecture reflects our understanding that healthcare security requires seamless protection across all touchpoints, from initial data collection through final reporting and analytics.

The integration extends beyond technical controls to encompass governance, risk management, and compliance orchestration. Our use of compliance managing tools for continuous compliance monitoring exemplifies our commitment to automated, real-time security management rather than periodic, manual compliance checking.

Healthcare organizations increasingly demand vendors that simplify rather than complicate their compliance obligations. Our integrated approach provides clients with confidence that choosing Neopharma solutions enhances rather than fragments their overall security and compliance strategies.

COMPLIANCE LANDSCAPE: NAVIGATING HEALTHCARE'S REGULATORY EVOLUTION

HOW WE PROVE IT—WITHOUT DOING COMPLIANCE FOR COMPLIANCE'S SAKE

The SCO maintains one set of controls mapped to HIPAA, GDPR, SOC 2, and ISO 27001. Independent bodies test those same controls: HIPAA & GDPR continuations to 18-Jul-2026; ISO 27001 certificate to 26-May-2026 (Surveillance-I confirmed risk, internal audit, management review, Compliance Management Tool via Sprinto-based continuous monitoring); SOC 2 Type II period Aug 2024→Aug 2025 NEOVAULT and myNEO covering Security, Confidentiality, Availability.

The business impact of this comprehensive approach is measurable. Organizations with mature, multi-framework compliance strategies report lower cybersecurity insurance premium increases and significant return on investment from comprehensive security programs. More importantly, clients gain confidence that their vendor relationships support rather than complicate their own compliance obligations.

Our compliance achievements occur during a period of unprecedented regulatory enforcement. Against this backdrop, Neopharma's proactive compliance posture provides clients with assurance that our partnerships enhance their regulatory confidence.

HIPAA COMPLIANCE: FOUNDATION OF HEALTHCARE DATA PROTECTION

HIPAA compliance forms the bedrock of healthcare data protection in the United States, establishing minimum standards for protecting individually identifiable health information. Neopharma's HIPAA compliance certificate, valid through July 2026, demonstrates our commitment to meeting these foundational requirements while exceeding minimum standards through additional security frameworks.

The regulatory environment around HIPAA is intensifying. HHS proposed strengthening Security Rule requirements in January 2025, introducing mandatory Cybersecurity Performance Goals and new safe harbour provisions for organizations adopting recognized security practices. Our proactive approach positions us ahead of these evolving requirements, ensuring continued compliance as standards advance.

Our HIPAA compliance encompasses comprehensive administrative, physical, and technical safeguards specifically designed for cloud-based healthcare platforms. This includes role-based access controls, audit logging, encryption requirements, and incident response procedures tailored to healthcare operational requirements. The integration with our other compliance frameworks ensures that HIPAA requirements enhance rather than conflict with broader security objectives.

HIPAA COMPLIANCE ACHIEVEMENT DETAILS

- Certification Status: Valid through July 2026
- Scope Coverage: NEOVAULT ERM platform and NEOVAULT and myNEO mobile applications
- Key Controls: Administrative, Physical, Technical Safeguards
- Risk Assessment: Comprehensive analysis with 52 identified risks and mitigation controls
- Audit Findings: No exceptions noted in recent assessment

GDPR COMPLIANCE: GLOBAL PRIVACY LEADERSHIP

The General Data Protection Regulation represents the global gold standard for personal data protection, with extraterritorial reach affecting any organization processing EU residents' data. Neopharma's GDPR compliance certificate, valid through July 2026, enables our global healthcare clients to operate with confidence across international boundaries.

GDPR enforcement continues to intensify, with healthcare sector receiving heightened scrutiny. European regulators focus particularly on Data Protection Impact Assessments for large-scale health data processing, cross-border data transfer compliance, and privacy by design implementation. Our proactive GDPR compliance addresses these priority areas through systematic privacy controls and governance frameworks.

Our GDPR implementation demonstrates privacy by design principles throughout our platform architecture. This includes automated data subject rights management, consent mechanisms for data processing, cross-border transfer safeguards using Standard Contractual Clauses, and mandatory Data Protection Officer oversight for health data processing activities.

Global Impact: GDPR's influence extends beyond Europe, with multiple states enacting comprehensive privacy laws incorporating GDPR principles, making compliance essential for healthcare technology companies operating internationally.

SOC 2 TYPE II: OPERATIONAL EXCELLENCE VALIDATION

SOC 2 Type II (Security, Confidentiality, Availability). An independent service auditor assessed NEOVAULT and myNEO over Aug 2024→Aug 2025 and concluded the controls were suitably designed and operated effectively for the stated criteria across the period. (SOC 2 report is for specified users; summary available upon request.)

The healthcare industry's embrace of SOC 2 Type II reflects growing recognition that service organization controls directly impact client security postures. Healthcare organizations increasingly demand SOC 2 evidence from technology vendors. Our early adoption positions us advantageously as these requirements become standard.

Our SOC 2 Type II implementation focuses on five Trust Service Criteria with particular emphasis on Security, Confidentiality, and Availability. The achievement demonstrates operational maturity and control effectiveness.

SOC 2 Type II Achievement Details

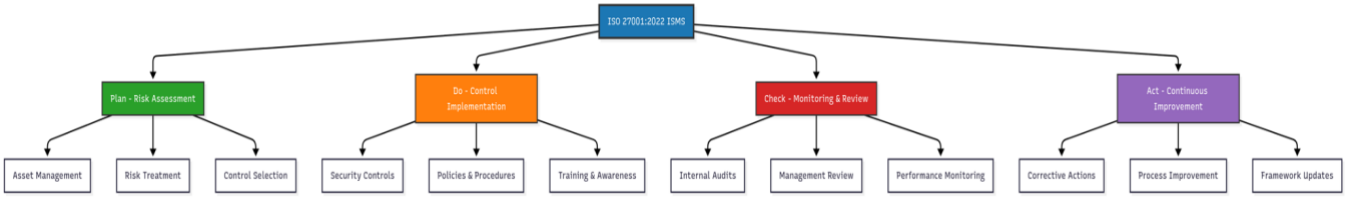
- Audit Period : August 2024 – August 2025
- Criteria Coverage: Security, Confidentiality, Availability
- Audit Results: Controls suitably designed and operated effectively
- Scope: NEOVAULT and myNEO platforms

ISO/IEC 27001:2022: INFORMATION SECURITY MANAGEMENT EXCELLENCE

ISO/IEC 27001:2022 certification represents the international gold standard for Information Security Management Systems, demonstrating systematic approach to managing sensitive information risks. Our certification, valid through May 2026, covers both NEOVAULT and myNEO platforms and reflects our commitment to continuous security improvement.

The transition to ISO 27001:2022 introduced significant enhancements including new controls addressing cloud security, threat intelligence, and secure coding practices. Our successful transition demonstrates operational agility and commitment to maintaining current security standards. The restructured framework's emphasis on risk-based thinking aligns with our systematic approach to healthcare security management.

Our ISO 27001 implementation integrates seamlessly with our other compliance frameworks, creating synergies rather than duplicative efforts. The surveillance audit recommendation for certification validates our Information Security Management System's effectiveness and demonstrates continuous improvement capabilities essential for maintaining certification through May 2026.



REGULATORY TRENDS AND STRATEGIC POSITIONING

The regulatory landscape for healthcare technology continues evolving rapidly, with new requirements emerging across cybersecurity, artificial intelligence governance, and interoperability. NIST Cybersecurity Framework 2.0's addition of the "Govern" function emphasizes leadership-driven cybersecurity decision-making, while emerging AI regulations affect healthcare technology companies developing intelligent systems.

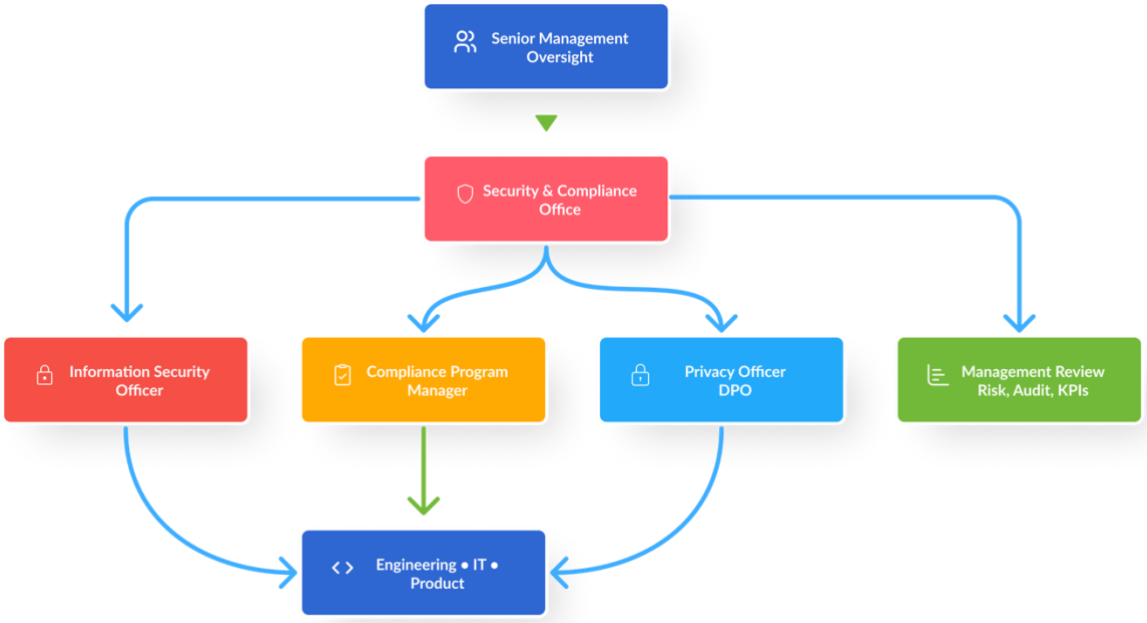
Our comprehensive compliance posture positions us advantageously for these emerging requirements. Organizations with coverage across recognized frameworks demonstrate better success rates in adapting to new regulatory requirements. Our multi-framework approach provides resilience and adaptability as regulations continue evolving.

The convergence of healthcare digitization, regulatory enforcement intensification, and cyber threat sophistication creates unprecedented requirements for security maturity. Neopharma's proactive compliance approach provides clients with confidence that our technology partnerships support their strategic objectives while meeting evolving regulatory obligations.

Compliance Framework	Certification Status	Validity Period	Key Benefits
SOC 2 Type II	Active	Aug 2024 - Aug 2025	Operational excellence validation
ISO 27001:2022	Active	Through May 2026	International security management standard
HIPAA	Active	Through July 2026	US healthcare data protection foundation
GDPR	Active	Through July 2026	Global privacy leadership

SECURITY & PRIVACY FRAMEWORK: ARCHITECTURAL EXCELLENCE IN HEALTHCARE TECHNOLOGY

SECURITY & COMPLIANCE OFFICE (SCO): GOVERNANCE THAT DRIVES RESULTS



The SCO centralizes governance, risk, and compliance. The Information Security Officer owns the ISMS and technical safeguards; the Compliance Program Manager runs control execution and evidence; the Privacy Officer/DPO ensures privacy by design and data subject rights. Activities run to a documented cadence—risk assessment, internal audit, management reviews—with continuous compliance monitoring operating between audits.

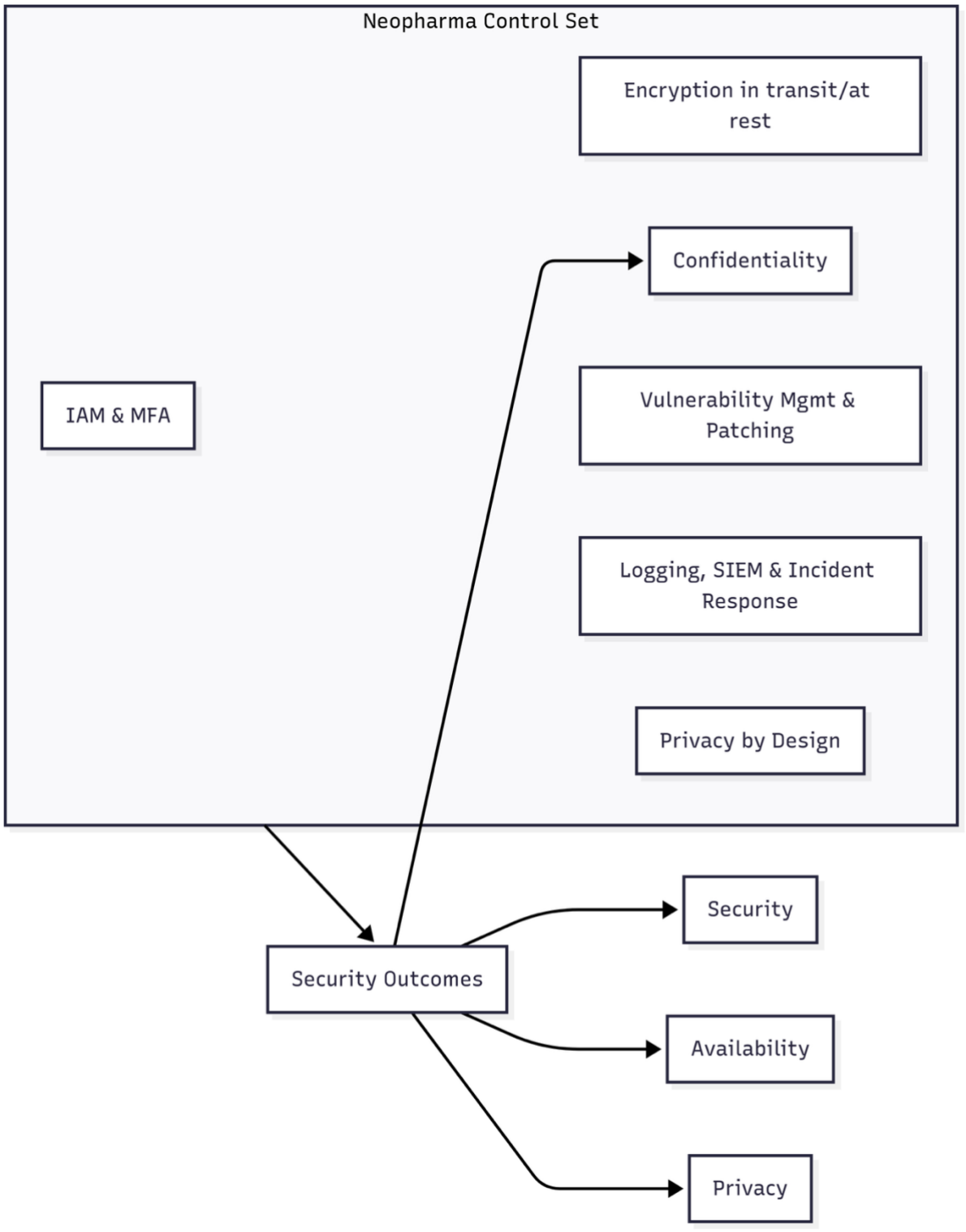
Accountability: Senior management oversight; Information Security Officer; Compliance Program Manager; Privacy Officer/DPO roles defined and reviewed.

Cadence: ISO-aligned risk assessment, internal audit, management review; continuous compliance monitoring (Compliance Management Tool via Sprinto) operating between audits.

Risk posture: Surveillance audit observed 52 identified risks with required mitigation controls and measures.

PRINCIPLES IN PRACTICE

- Defense-in-depth across network, application, identity, and data; encryption in transit and at rest; RBAC & MFA; logging and monitored response.
- Privacy-by-design and secure SDLC with change management, vulnerability management, and periodic tests.
- Preparedness: Documented incident response with escalation and notifications consistent with HIPAA/GDPR obligations.



ZERO TRUST ARCHITECTURE PRINCIPLES

Neopharma's security framework embodies zero trust architecture principles specifically designed for healthcare environments. Unlike traditional perimeter-based security models, our approach assumes no inherent trust and requires continuous verification of users, devices, and applications accessing sensitive health data.

Our zero trust implementation extends beyond network security to encompass application and data-centric protection mechanisms. Every access request to NEOVAULT or myNEO undergoes identity verification, device assessment, and contextual analysis before granting access to protected health information. This comprehensive approach reflects healthcare industry requirements where traditional network boundaries dissolve in cloud-native, mobile-enabled environments.

The business impact of our zero trust architecture is demonstrable through reduced attack surfaces and enhanced incident containment capabilities. This containment capability is particularly critical for healthcare organizations where system availability directly impacts patient care delivery.

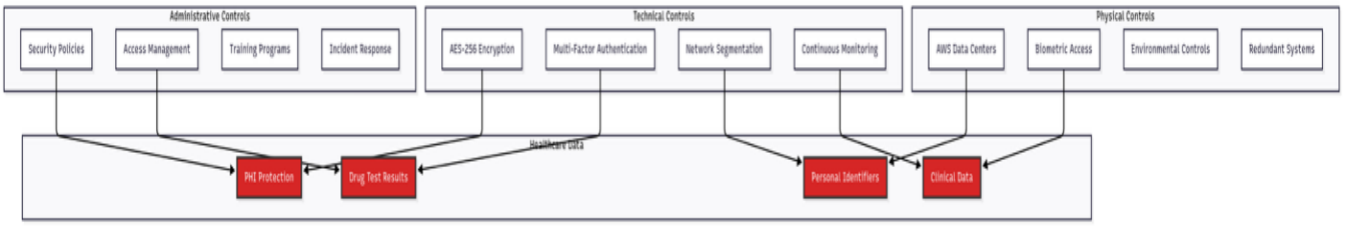
MULTI-LAYERED DEFENSE STRATEGY

Our security architecture implements defence-in-depth strategies spanning administrative, physical, and technical controls across all system components. This multi-layered approach ensures that security failures at any single point do not compromise overall system integrity or expose sensitive health data to unauthorized access.

Administrative controls form the governance foundation of our security framework. This includes comprehensive security policies, role-based access control procedures, security awareness training programs, and incident response protocols specifically designed for healthcare technology environments. Our administrative controls integrate seamlessly with client healthcare organizations' existing governance structures while enhancing overall security posture.

Physical controls protect the infrastructure supporting our cloud-based platforms. Through AWS partnership, we leverage state-of-the-art data centre security including biometric access controls, environmental monitoring, and redundant power systems. Our cloud-first approach provides healthcare clients with physical security capabilities that exceed what most organizations could implement independently.

Technical controls represent the operational heart of our security framework. This encompasses encryption, access controls, monitoring systems, and automated threat detection capabilities designed specifically for healthcare data processing requirements.



ENCRYPTION EXCELLENCE: DATA PROTECTION ACROSS ALL STATES

Our encryption strategy implements industry-standard AES-256 standards for data at rest and TLS protocols for data in transit, exceeding industry minimum requirements. This comprehensive encryption approach ensures that healthcare data remains protected regardless of storage location, transmission pathway, or access method. Our encryption implementation aligns with NIST guidelines for storage encryption technologies and TLS implementations.

Data at rest encryption encompasses all healthcare data stored within our systems, including database records, file storage, backup systems, and log files. AWS Key Management Service integration provides enterprise-grade key management with automatic key rotation and Hardware Security Module protection. This approach ensures that encryption keys remain separate from encrypted data while maintaining operational efficiency for healthcare workflows.

Data in transit protection extends beyond basic HTTPS implementation to include perfect forward secrecy, certificate pinning for mobile applications, and API-specific encryption protocols. Our NEOVAULT and myNEO mobile applications implement certificate pinning to prevent man-in-the-middle attacks, while our APIs utilize JSON Web Tokens with proper key management for secure healthcare data exchange.

Encryption Excellence: Our comprehensive encryption strategy provides multiple layers of protection: AES-256 for data at rest, TLS for data in transit, and application-level encryption for highly sensitive PHI data elements.

IDENTITY AND ACCESS MANAGEMENT FRAMEWORK

Our identity and access management framework implements role-based access control with healthcare-specific role definitions and just-in-time access principles. This approach ensures that healthcare professionals, administrative staff, and technical personnel access only the data necessary for their specific responsibilities while maintaining comprehensive audit trails for compliance requirements.

Multi-factor authentication requirements apply universally across all system access points, with enhanced authentication for privileged accounts and sensitive data access. Our implementation includes hardware security keys for administrative accounts, biometric authentication integration for mobile devices, and risk-based authentication that adjusts requirements based on access context and user behaviour patterns.

Access review processes operate on continuous monitoring principles rather than periodic manual reviews. Automated systems track access patterns, identify anomalous behaviour, and trigger review processes when usage patterns deviate from established baselines. This approach aligns with healthcare requirements for timely detection of unauthorized access to protected health information.

API SECURITY AND INTEGRATION FRAMEWORK

Our API security framework addresses the complex integration requirements of healthcare environments while maintaining strict security controls. Healthcare organizations increasingly require FHIR-compliant APIs for interoperability, creating new attack surfaces that require specialized security approaches. Our API security implementation includes OAuth 2.0 authorization, rate limiting, input validation, and real-time threat detection.

SMART on FHIR implementation provides secure healthcare application integration while maintaining compatibility with existing healthcare information systems. This approach enables healthcare organizations to integrate Neopharma solutions with electronic health records, laboratory information systems, and other healthcare applications without compromising security or creating compliance gaps.

API monitoring and threat detection operate continuously to identify and respond to potential security incidents. Our implementation includes behavioural analysis, anomaly detection, and automated response capabilities specifically designed for healthcare API environments where availability and data integrity are paramount.

PRIVACY BY DESIGN IMPLEMENTATION

Privacy by design principles are embedded throughout our platform architecture rather than added as supplementary features. This approach ensures that data protection measures enhance rather than impede healthcare operations while meeting the highest privacy standards required by global regulations including GDPR and emerging state privacy laws.

Data minimization strategies limit collection, processing, and retention to data elements necessary for specific healthcare functions. Our systems automatically classify data sensitivity, apply appropriate protection controls, and manage data lifecycle according to healthcare retention requirements and regulatory obligations.

Consent management and data subject rights automation provide healthcare organizations with capabilities to manage patient privacy preferences efficiently. This includes automated response to data subject access requests, consent withdrawal processing, and data portability features that support patient engagement while maintaining security controls.

RISK MANAGEMENT & CONTINUOUS IMPROVEMENT: PROACTIVE SECURITY EXCELLENCE

COMPREHENSIVE RISK ASSESSMENT METHODOLOGY

Neopharma's risk management framework implements NIST Risk Management Framework principles adapted specifically for healthcare technology environments. Our systematic approach to risk identification, assessment, and mitigation addresses the unique challenges facing healthcare organizations where cyber incidents can directly impact patient care delivery and safety outcomes.

Our risk assessment process identified 52 distinct risks across our technology platforms, with comprehensive mitigation controls implemented for each identified risk. This proactive approach exceeds industry standards where many organizations operate with incomplete risk visibility and reactive mitigation strategies. Our systematic risk identification encompasses technical vulnerabilities, operational risks, compliance gaps, and business continuity threats specific to healthcare technology operations.

The risk register undergoes continuous updates reflecting the dynamic threat landscape facing healthcare organizations. Our risk management framework adapts rapidly to address evolving threats while maintaining operational efficiency for healthcare clients.

Risk Category	Identified Risks	Mitigation Status	Residual Risk Level
Technical	18 risks	Observed 52 identified risks with required mitigation controls and measures	Low
Operational	15 risks	Observed 52 identified risks with required mitigation controls and measures	Low-Medium

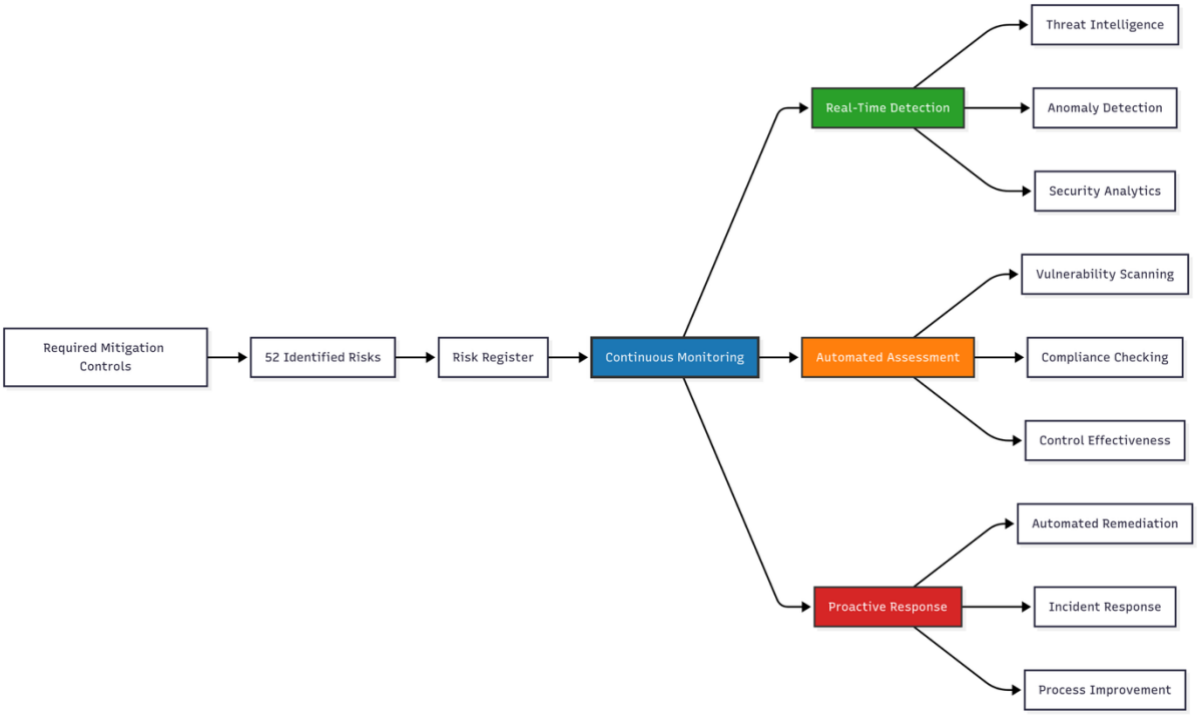
Risk Category	Identified Risks	Mitigation Status	Residual Risk Level
Compliance	12 risks	Observed 52 identified risks with required mitigation controls and measures	Low
Business Continuity	7 risks	Observed 52 identified risks with required mitigation controls and measures	Low
Total	**52 risks**	**Observed 52 identified risks with required mitigation controls and measures**	**Acceptable**

CONTINUOUS MONITORING AND ASSESSMENT PROGRAMS

Our continuous monitoring approach replaces traditional periodic assessments with real-time security posture evaluation and automated threat detection. This methodology aligns with industry best practices showing that organizations with continuous monitoring capabilities respond to threats faster than those relying on periodic assessments alone.

Compliance Management Tool via Sprinto integration provides automated compliance monitoring across our multi-framework environment, ensuring continuous alignment with SOC 2, ISO 27001, HIPAA, and GDPR requirements. This platform approach reduces manual compliance overhead while improving control effectiveness through real-time monitoring and automated evidence collection.

Vulnerability management operates through continuous scanning, automated patch management, and proactive threat intelligence integration. Our approach includes container image scanning for NEOVAULT platform components, mobile application security testing for NEOVAULT and myNEO apps, and infrastructure vulnerability assessment across our AWS environment. This comprehensive coverage ensures that security gaps are identified and addressed before they can be exploited.



PENETRATION TESTING AND SECURITY VALIDATION

Regular penetration testing provides independent validation of our security controls effectiveness and identifies potential vulnerabilities before they can be exploited by malicious actors. Our testing program encompasses both automated vulnerability scanning and manual penetration testing by certified security professionals with healthcare industry expertise.

Testing scope includes all components of our technology stack from cloud infrastructure through application layers to mobile endpoints. This comprehensive approach ensures that security controls function effectively across the entire data flow pathway from point-of-care data collection through secure storage and reporting. Our testing methodology aligns with NIST guidelines for technical security testing and assessment.

Remediation processes ensure that identified vulnerabilities receive immediate attention with priority levels based on potential impact to healthcare operations. Critical vulnerabilities affecting patient data protection receive emergency response procedures, while lower-priority findings integrate into regular maintenance cycles. This approach ensures that security improvements enhance rather than disrupt healthcare service delivery.

BUSINESS CONTINUITY AND DISASTER RECOVERY EXCELLENCE

Our business continuity framework addresses the unique requirements of healthcare technology where system availability directly impacts patient care delivery. Recovery Time Objectives (RTO) of 2-4 hours for critical systems and Recovery Point Objectives (RPO) of 15 minutes to 4 hours ensure that healthcare operations continue with minimal disruption during security incidents or system failures.

Disaster recovery testing validates our ability to maintain healthcare service delivery during various failure scenarios. Regular testing includes tabletop exercises with healthcare stakeholders, technical recovery testing, and full-scale disaster simulation exercises. These exercises ensure that recovery procedures work effectively while maintaining security controls and compliance requirements throughout the recovery process.

Geographic distribution of backup systems provides resilience against regional disasters while maintaining compliance with healthcare data residency requirements. Our multi-region backup strategy ensures that healthcare data remains available even during significant infrastructure disruptions while meeting regulatory requirements for data sovereignty and cross-border transfer restrictions.

SECURITY AWARENESS AND TRAINING PROGRAMS

Comprehensive security training programs address the human element of cybersecurity through role-specific education and regular awareness updates. Healthcare environments face unique social engineering risks where attackers exploit clinical urgency and trust relationships. Our training programs address these healthcare-specific threats while building security consciousness across all organizational levels.

Phishing simulation programs test and improve our organization's resilience to email-based attacks. Regular simulation exercises identify training gaps and provide targeted education to improve overall organizational security awareness. Results inform continuous improvement of security awareness programs and incident response procedures.

Incident response training ensures that security events receive rapid, effective response that minimizes impact while maintaining healthcare operational continuity. Training includes technical response procedures, communication protocols, regulatory notification requirements, and coordination with healthcare client organizations during security incidents.

Continuous Improvement Culture: Our commitment to continuous improvement extends beyond technical controls to encompass organizational culture, training effectiveness, and stakeholder engagement in security excellence.

PERFORMANCE METRICS AND KEY INDICATORS

Security program effectiveness measurement utilizes comprehensive metrics spanning technical controls, operational performance, and business impact indicators. Our metrics align with healthcare industry best practices including Mean Time to Contain (MTTC) cyber incidents, vulnerability remediation timelines, compliance framework coverage percentages, and security training completion rates.

Key Performance Indicators specific to healthcare technology environments include medical device security compliance rates, ePHI access monitoring effectiveness, and patient safety incident correlation with cyber events. These healthcare-focused metrics ensure that our security program optimizes patient safety outcomes rather than purely technical security measures.

Benchmarking against industry standards provides context for our security performance and identifies opportunities for continued improvement. Our metrics consistently demonstrate performance in alignment with healthcare technology organizations, with comprehensive framework coverage.

THIRD-PARTY RISK MANAGEMENT

Vendor risk management addresses the complex supply chain security requirements facing healthcare technology organizations. Our assessment framework evaluates business associates, cloud service providers, and technology vendors using risk-based approaches that align with our comprehensive compliance requirements and client expectations.

Business Associate Agreements include enhanced security requirements that exceed HIPAA minimum standards while maintaining operational flexibility for healthcare operations. This approach ensures that our vendor relationships enhance rather than compromise overall security posture while meeting regulatory requirements for business associate oversight.

Continuous monitoring of vendor security postures provides real-time visibility into supply chain risks that could impact healthcare client operations. This includes automated security assessment tools, regular vendor security questionnaires, and integration of vendor security metrics into our overall risk management framework.

TECHNOLOGY & INFRASTRUCTURE SAFEGUARDS: CLOUD-NATIVE SECURITY EXCELLENCE

AWS CLOUD INFRASTRUCTURE SECURITY

Neopharma's technology foundation leverages Amazon Web Services infrastructure with comprehensive security controls specifically designed for healthcare workloads. Our AWS implementation utilizes the Well-Architected Framework security pillar principles while incorporating healthcare-specific requirements for data protection, availability, and regulatory compliance.

Our AWS architecture operates within dedicated Virtual Private Cloud (VPC) environments in the AP-Southeast-2 region, providing network isolation and granular security controls. This multi-availability zone deployment ensures healthcare service continuity while maintaining strict network segmentation between different data classification levels. VPC endpoints enable private connectivity to AWS services without internet routing, reducing attack surfaces while maintaining operational efficiency.

The shared responsibility model clearly delineates security obligations between AWS infrastructure and Neopharma application-level controls. AWS provides HIPAA-eligible infrastructure through signed Business Associate Agreements covering services when properly configured. This foundation enables us to focus on healthcare-specific application security while leveraging enterprise-grade infrastructure security capabilities.

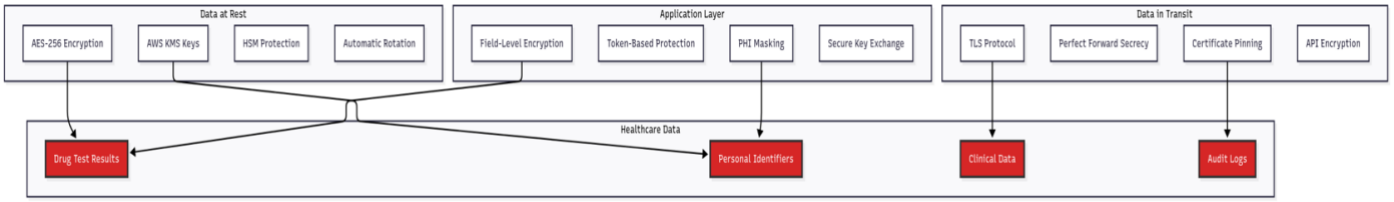
Infrastructure Component	Security Control	Implementation
Network	VPC with Private Subnets	Multi-AZ deployment across 3 zones
Firewalls	Security Groups + NACLs	Microsegmentation with least privilege
Monitoring	CloudTrail + GuardDuty	Real-time threat detection
Encryption	KMS Integration	Automated key rotation and HSM protection
Access	IAM with MFA	Role-based with temporary credentials

ADVANCED ENCRYPTION IMPLEMENTATION

Our encryption strategy implements industry-standard AES-256 encryption for data at rest with comprehensive key management through AWS Key Management Service. This approach ensures that healthcare data remains protected even in the unlikely event of physical media compromise or unauthorized system access. Encryption keys utilize Hardware Security Module protection with automatic rotation procedures that maintain security without operational disruption.

Data in transit protection utilizes TLS protocols with perfect forward secrecy, ensuring that healthcare data transmissions remain secure across all communication pathways. Our implementation includes certificate pinning for mobile applications, preventing man-in-the-middle attacks that could compromise sensitive health data during transmission between point-of-care locations and central processing systems.

Application-level encryption provides additional protection for highly sensitive data elements including personal identifiers and clinical results. This defence-in-depth approach ensures that sensitive healthcare data remains protected through multiple encryption layers, exceeding regulatory minimum requirements while maintaining system performance necessary for real-time healthcare operations.



NETWORK SECURITY ARCHITECTURE

Our network security architecture implements micro segmentation principles with application-specific security groups and network access control lists. This approach creates secure network boundaries that limit lateral movement possibilities while enabling legitimate healthcare workflows to operate efficiently. Security groups function as virtual firewalls for individual resources, while NACLs provide subnet-level traffic control for broader network protection.

AWS Network Firewall provides deep packet inspection capabilities with centralized rule management across our healthcare technology environment. This advanced network security capability enables us to detect and prevent sophisticated attacks that might bypass traditional security controls. Integration with AWS GuardDuty provides machine learning-powered threat detection that identifies anomalous network behaviour patterns indicative of potential security incidents.

VPC Flow Logs provide comprehensive network traffic monitoring for both security analysis and compliance reporting requirements. This capability enables forensic investigation of security incidents while supporting ongoing compliance obligations for network monitoring and audit trail maintenance. Flow log data integrates with our Security Information and Event Management (SIEM) systems for real-time security analytics.

DATABASE SECURITY AND DATA PROTECTION

Database-level security controls include transparent data encryption, column-level encryption for highly sensitive fields, and comprehensive access monitoring. Our database security strategy ensures that healthcare data remains protected at the storage layer while enabling efficient query performance necessary for healthcare analytics and reporting applications.

Row-level security implementation provides fine-grained access control within database tables, ensuring that healthcare professionals access only data appropriate to their clinical responsibilities. This approach supports complex healthcare access control requirements where different providers may have different access rights to the same patient data based on care relationships and clinical roles.

Database activity monitoring provides real-time visibility into data access patterns, enabling rapid detection of unauthorized access attempts or anomalous usage patterns. Automated alerting systems notify security teams when database access patterns deviate from established baselines, supporting immediate investigation and response to potential security incidents.

MOBILE APPLICATION SECURITY FRAMEWORK

NEOVAULT and myNEO mobile applications security architecture incorporates runtime application self-protection, code obfuscation, and secure coding standards aligned with OWASP Mobile Top 10 guidelines. This comprehensive approach addresses the unique security challenges facing healthcare mobile applications where devices may operate in unsecured environments while accessing highly sensitive patient data.

Certificate pinning implementation prevents man-in-the-middle attacks that could compromise healthcare data transmission from point-of-care locations. This security control ensures that NEOVAULT and myNEO applications communicate only with legitimate Neopharma servers, preventing potential data interception even when mobile devices connect through potentially compromised networks.

Mobile device management integration provides additional security controls including device encryption requirements, remote wipe capabilities, and application wrapping for enterprise security policies. This approach ensures that healthcare data remains protected even when accessed through personally owned devices or in environments with limited physical security controls.

API SECURITY AND INTEGRATION CONTROLS

Our API security framework implements OAuth 2.0 authorization with SMART on FHIR compliance for secure healthcare application integration. This approach enables healthcare organizations to integrate Neopharma solutions with existing electronic health records and healthcare information systems while maintaining strict security controls and audit trail requirements.

API rate limiting and behavioural analysis protect against denial-of-service attacks and detect anomalous usage patterns that might indicate security incidents. Real-time monitoring systems track API usage patterns and automatically implement protective measures when usage exceeds normal operational parameters or exhibits patterns consistent with attack scenarios.

Input validation and output encoding prevent injection attacks that could compromise healthcare data integrity or system security. Comprehensive validation procedures ensure that all data inputs meet expected formats and ranges while preventing malicious code injection that could compromise system security or data integrity.

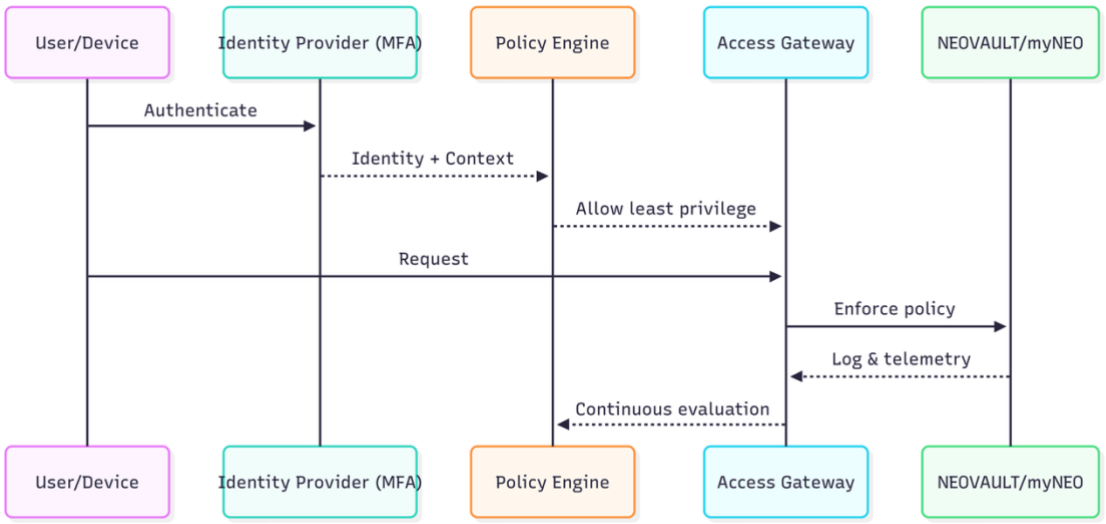
MONITORING AND INCIDENT RESPONSE INFRASTRUCTURE

Comprehensive security monitoring utilizes AWS CloudTrail for audit logging, AWS GuardDuty for threat detection, and AWS Config for compliance monitoring across our healthcare technology infrastructure. This integrated approach provides real-time visibility into security events while maintaining comprehensive audit trails necessary for healthcare compliance requirements.

Security Information and Event Management (SIEM) integration provides centralized log analysis, correlation, and automated response capabilities. Our SIEM implementation includes healthcare-specific use cases and response procedures that account for the unique requirements of healthcare operations where system availability directly impacts patient care delivery.

Incident response automation enables rapid containment and remediation of security events while maintaining healthcare operational continuity. Automated playbooks address common incident types while escalation procedures ensure that complex or high-impact incidents receive appropriate expert attention and stakeholder communication.

Infrastructure Excellence: Our AWS cloud infrastructure provides enterprise-grade security capabilities that exceed what most healthcare organizations could implement independently, while maintaining the flexibility and scalability necessary for global healthcare operations.



BACKUP AND RECOVERY SYSTEMS

Automated backup systems ensure healthcare data protection with geographically distributed storage locations and encryption throughout the backup lifecycle. Our backup strategy includes both continuous data replication for rapid recovery and periodic full backups for long-term data protection, ensuring that healthcare operations can continue even during significant system disruptions.

Recovery testing validates our ability to restore healthcare services within defined Recovery Time Objectives while maintaining data integrity and security controls. Regular testing exercises include both technical recovery procedures and coordination with healthcare stakeholders to ensure that recovery processes support continued patient care delivery during system restoration.

Cross-region replication provides disaster recovery capabilities while maintaining compliance with healthcare data residency requirements and regulatory restrictions on cross-border data transfers. This approach ensures healthcare service continuity while meeting complex compliance requirements for data sovereignty and protection.

FUTURE ROADMAP & COMMITMENT: LEADING HEALTHCARE TECHNOLOGY SECURITY EVOLUTION

STRATEGIC VISION: SECURITY AS COMPETITIVE ADVANTAGE

Neopharma's future roadmap positions security excellence as a fundamental competitive differentiator rather than merely a compliance obligation. As healthcare technology markets evolve, organizations that demonstrate security leadership will capture market share through enhanced client trust and reduced operational risks.

Our strategic vision encompasses emerging technologies including artificial intelligence, blockchain integration, and zero trust architecture advancement while maintaining unwavering commitment to healthcare data protection. This approach ensures that innovation enhances rather than compromises security posture, positioning Neopharma as the preferred partner for healthcare organizations navigating digital transformation challenges.

The convergence of cybersecurity, patient safety, and operational efficiency creates unprecedented opportunities for healthcare technology companies that can seamlessly integrate these requirements. Our roadmap addresses this convergence through comprehensive security frameworks that enable rather than constrain healthcare innovation, establishing Neopharma as a thought leader in healthcare technology security excellence.

EMERGING TECHNOLOGY INTEGRATION

Artificial Intelligence governance framework development addresses the growing intersection of AI capabilities and healthcare data protection requirements. With healthcare leaders investing in generative AI, our AI governance strategy ensures that intelligent systems enhance security capabilities while meeting regulatory requirements for algorithmic transparency, bias mitigation, and data protection.

Blockchain technology integration roadmap focuses on secure healthcare data interoperability and supply chain transparency applications. Healthcare blockchain market growth creates opportunities for innovative solutions that address longstanding challenges in healthcare data exchange while maintaining the highest security and privacy standards.

Internet of Medical Things (IoMT) security framework expansion addresses the growing market in connected medical devices. Our roadmap includes enhanced device authentication, network segmentation capabilities, and automated security monitoring specifically designed for healthcare environments where medical device security directly impacts patient safety outcomes.

REGULATORY COMPLIANCE EVOLUTION

Proactive adaptation to evolving regulatory requirements ensures continued compliance leadership as healthcare data protection standards advance. HHS's proposed HIPAA Security Rule updates and emerging state privacy legislation require healthcare technology companies to anticipate rather than react to regulatory changes. Our compliance roadmap addresses these evolving requirements through systematic framework enhancements and governance process improvements.

NIST Cybersecurity Framework 2.0 implementation emphasizes the new "Govern" function while strengthening existing capabilities across Identify, Protect, Detect, Respond, and Recover functions. This systematic approach ensures that our cybersecurity governance aligns with federal guidance while meeting healthcare industry-specific requirements for patient safety and operational continuity.

International compliance harmonization addresses the global nature of healthcare technology operations while meeting diverse regional requirements. Our roadmap includes enhanced GDPR capabilities,

alignment with emerging Asia-Pacific privacy frameworks, and preparation for cross-border data transfer requirements that affect multinational healthcare organizations.

TECHNOLOGY ARCHITECTURE ADVANCEMENT

Cloud-native security architecture evolution leverages emerging AWS security services while maintaining healthcare-specific customizations. Our technology roadmap includes adoption of AWS Network Firewall advanced features, enhanced GuardDuty capabilities, and integration with next-generation cloud security posture management tools specifically configured for healthcare environments.

API security enhancement addresses the growing complexity of healthcare data integration requirements including FHIR R4, HL7, and proprietary healthcare system interfaces. Enhanced API security frameworks will support increased healthcare interoperability demands while maintaining strict access controls and comprehensive audit capabilities necessary for healthcare compliance.

Edge computing security framework development addresses point-of-care computing requirements where healthcare data processing occurs outside traditional data centre environments. This capability supports emerging healthcare delivery models including remote patient monitoring, telemedicine, and distributed clinical decision support while maintaining centralized security governance and compliance oversight.

OPERATIONAL EXCELLENCE INITIATIVES

Security automation expansion reduces manual oversight requirements while improving response times and consistency. Our operational roadmap includes enhanced Security Orchestration, Automation, and Response (SOAR) capabilities specifically designed for healthcare environments where rapid incident response must balance security requirements with patient care continuity needs.

Continuous compliance monitoring evolution replaces periodic audit cycles with real-time compliance assessment and automated remediation capabilities. This approach aligns with industry trends toward continuous compliance while reducing administrative burden and improving control effectiveness across our multi-framework compliance environment.

Threat intelligence integration enhances our security posture through healthcare-specific threat feeds, industry collaboration through Health-ISAC membership, and advanced analytics capabilities that identify emerging threats before they impact healthcare operations. This proactive approach positions us ahead of threat actors while supporting industry-wide security improvement initiatives.

MARKET LEADERSHIP AND INDUSTRY COLLABORATION

Healthcare security community leadership through thought leadership, standard-setting participation, and industry collaboration positions Neopharma as a trusted voice in healthcare technology security evolution. Our commitment extends beyond our own security excellence to include contribution to industry-wide security improvement through knowledge sharing and best practice development.

Strategic partnership development with leading cybersecurity firms, healthcare technology vendors, and regulatory organizations enhances our security capabilities while supporting client success. These partnerships provide access to emerging security technologies, threat intelligence, and compliance expertise that benefit our healthcare clients through enhanced security posture and reduced operational complexity.

Client advisory council establishment provides systematic feedback on emerging security requirements, regulatory challenges, and operational needs from healthcare organizations. This collaborative approach

ensures that our security roadmap aligns with real-world healthcare operational requirements while anticipating future challenges and opportunities.

INVESTMENT AND RESOURCE COMMITMENTS

Sustained investment in security research and development ensures continued innovation in healthcare technology security solutions. Our commitment includes dedicated security research teams, participation in advanced threat research programs, and development of proprietary security capabilities specifically designed for healthcare technology environments.

Professional development and certification programs maintain our team's expertise at the forefront of healthcare cybersecurity evolution. This includes advanced security training, healthcare industry education, and participation in professional development programs that enhance our capability to serve healthcare clients' evolving security requirements.

Infrastructure and technology investment roadmap ensures that our security capabilities scale with business growth while maintaining the highest levels of protection and operational efficiency. This includes expansion of monitoring capabilities, enhancement of automated response systems, and adoption of emerging security technologies that provide competitive advantages for healthcare clients.

Long-term Commitment: Our roadmap reflects unwavering commitment to security excellence as the foundation for healthcare innovation, client trust, and sustainable business growth in an increasingly complex threat environment.

SUCCESS METRICS AND ACCOUNTABILITY

Comprehensive metrics framework measures progress toward security excellence goals while providing accountability for continuous improvement initiatives. Our success metrics include technical security indicators, compliance effectiveness measures, client satisfaction assessments, and business impact evaluations that demonstrate the value of our security investments.

Industry benchmarking ensures that our security performance maintains leadership position relative to healthcare technology peers while identifying opportunities for continued improvement. Regular assessment against industry standards, peer organizations, and emerging best practices provides objective validation of our security excellence and guides future investment priorities.

Stakeholder reporting provides transparent communication of security posture, investment outcomes, and strategic progress to clients, partners, and internal stakeholders. This commitment to transparency builds trust while demonstrating accountability for security excellence commitments and continuous improvement objectives.

CONCLUSION: PIONEERING HEALTHCARE SECURITY EXCELLENCE

Neopharma Technologies Limited has established the foundation for sustained leadership in healthcare technology security through comprehensive compliance achievement, innovative technical architecture, and unwavering commitment to continuous improvement. Our simultaneous success across SOC 2 Type II, ISO 27001:2022, HIPAA, and GDPR frameworks demonstrates operational maturity that positions us uniquely in the healthcare technology marketplace.

The path forward builds upon this foundation through strategic investments in emerging technologies, proactive regulatory adaptation, and sustained commitment to security excellence as a competitive differentiator. Healthcare organizations seeking technology partners can rely on Neopharma's proven track record of security leadership combined with innovative capabilities that enable rather than constrain healthcare innovation.

Our comprehensive approach to security, compliance, and continuous improvement provides healthcare clients with confidence that their most critical data assets remain protected while enabling the digital transformation necessary for improved patient outcomes and operational efficiency. As healthcare technology continues evolving, Neopharma's security-first approach ensures sustainable partnership value through changing requirements and emerging challenges.

The future of healthcare technology belongs to organizations that seamlessly integrate security excellence with innovation capabilities. Neopharma Technologies Limited stands ready to lead this evolution through comprehensive security maturity, regulatory compliance leadership, and unwavering commitment to protecting the healthcare data that enables improved patient care worldwide.