NexaCareTech Privacy, Security & Data Protection Framework

Protecting Client Data. Protecting Agencies. Protecting Trust.

Version 1.0 | Effective Date: October 2026

Applies to: NexaCareTech LLC, its workforce, contractors, developers, vendors, systems, applications, and third-party integrations.

Document title	Privacy, Security & Data Protection Framework
Owner	Chief Technology Officer, NexaCareTech LLC
Version	1.1
Effective date	4 October 2026
Review cycle	Annually, and upon any material change to the environment
Classification	Internal — not for distribution outside NexaCareTech LLC
Related document	NexaCareTech Launch Readiness and Security Roadmap

Status of this Document

This Framework is a statement of the internal policies, standards and controls adopted by NexaCareTech LLC ("NexaCareTech", "the Company") for the protection of information entrusted to the NexaCareTech platform. It is issued under the authority of the Company and applies to the Company's workforce, contractors, developers, vendors, systems, applications and third-party integrations.

Compliance with this Framework is mandatory for all persons to whom it applies. Access to Company systems is conditional upon adherence to it. Failure to comply may result in withdrawal of access, termination of engagement, and such further action as the Company considers appropriate.

This Framework does not create rights in favour of any third party, and does not vary, limit or supersede any Business Associate Agreement, customer agreement, vendor agreement or other binding instrument to which the Company is party. Where a conflict arises between this Framework and such an instrument, the instrument prevails to the extent of the conflict and the matter shall be escalated to the document owner for resolution.

Where this Framework states that a control "should" be implemented, that control represents the Company's intended standard and its implementation is governed by the related Launch Readiness and Security Roadmap. Where this Framework states that a control "must" be implemented, that control is mandatory and no exception applies without documented approval by the document owner.

The current implementation status of the controls described here is recorded separately in the Launch Readiness and Security Roadmap, which is maintained as a living document and updated as work completes.

Nothing in this Framework constitutes legal advice. Determination of the laws and regulations applicable to any particular activity of the Company remains a matter for qualified counsel.

1. Purpose and Commitment

NexaCareTech will maintain a comprehensive data protection and privacy program designed to protect the confidentiality, integrity, availability, and lawful use of information entrusted to the platform.

Because NexaCareTech support home-care agencies with potentially sensitive health and personal information, security and privacy are core product requirements not an IT add-on.

- Privacy by Design
- Security by Design
- Least-Privilege Access
- Minimum Necessary Data
- Encryption by Default
- Continuous Monitoring
- Documented Accountability
- Rapid Incident Response
- Secure Third-Party Integration
- Regular Risk Assessment and Improvement

2. Regulatory and Compliance Framework

Primary Framework

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Breach Notification Rule
- HITECH Act
- Applicable federal data-security requirements
- Business Associate Agreements where NexaCareTech qualifies as a Business Associate

Minnesota

- Minnesota Health Records Act
- Minnesota breach-notification requirements
- Minnesota Consumer Data Privacy Act, where applicable
- Other applicable Minnesota privacy and security requirements
- Contractual requirements imposed by Minnesota healthcare programs and partners

Contractual / Industry

- Customer Business Associate Agreements

- HHAeXchange security/integration requirements
- Waystar requirements
- Cloud-service provider agreements
- Payment/billing partner requirements
- EVV-related contractual requirements
- Vendor security requirements

Legal counsel should determine exactly which laws apply to each NexaCareTech business activity. This document establishes NexaCareTech operational security framework and does not substitute for legal advice.

3. Data Classification

Classification	Examples	Protection
Public	Website content, marketing materials	Standard controls
Internal	Internal procedures, business documents	Restricted employee access
Confidential	Contracts, financial information, employee information	Encryption + access controls
Sensitive Personal Data	Names, addresses, phone numbers, IDs	Strong access restrictions
PHI/ePHI	Client health information, care plans, diagnoses, services	Highest protection
Highly Restricted	Passwords, encryption keys, credentials, tokens	Strict privileged access

Special categories include client demographics, health information, care plans, medication information, service documentation, EVV records, caregiver information, financial/billing information, insurance information, Medicaid/MHCP information, identifiers, authentication credentials, API keys, access tokens, audit logs, location information, device information, and uploaded documents.

4. Data Ownership and Roles

Customer Data

Information uploaded or generated by a home-care agency through NexaCareTech. Generally, the customer should retain ownership/control of its customer data, subject to the contractual relationship and applicable law.

NexaCareTech Operational Data

Information NexaCareTech requires to operate, secure, maintain, and improve the platform, subject to contractual restrictions.

System Security Data

Security logs, authentication records, audit trails, IP addresses, device identifiers, and security alerts should be clearly defined, with documented collection, use, access, and retention rules.

5. Privacy-by-Design Principles

1. What data does the feature collect?
2. Why is the data required?
3. Is every data element necessary?
4. Who needs access?
5. What happens if the data is compromised?
6. How long should it be retained?
7. Does the feature transmit data to another organization?
8. Does it create a new HIPAA or contractual obligation?
9. Does it involve a new vendor or API?
10. Can the feature be designed to use less identifiable information?

Significant new functionality should undergo a documented Privacy Impact Assessment (PIA) and/or Security Impact Assessment before production release.

6. Access Control

NexaCareTech will implement Role-Based Access Control (RBAC). Users should only see information necessary for their job.

Role	Typical Access
Agency Administrator	Agency-wide operational information
Scheduler	Scheduling/client information needed for scheduling
Caregiver	Assigned client/service information
Billing Staff	Billing and claims information
Supervisor	Appropriate client/caregiver information
Agency Owner	Authorized agency-wide information
NexaCare Support	Restricted support access
NexaCare Developer	No routine production PHI access
Security Administrator	Security administration
System Administrator	Infrastructure access subject to strict controls

7. Authentication

- Unique user IDs
- Strong password requirements
- Multi-factor authentication (MFA)
- Session timeout
- Account lockout/rate limiting
- Secure password reset
- Device/session management

- Login monitoring
- Protection against credential stuffing and brute-force attacks

MFA should be mandatory for developers, database administrators, cloud administrators, security administrators, company administrators, and production-support personnel. Privileged users should have separate administrative accounts.

8. Encryption

Data in Transit

Use modern TLS for the web application, mobile applications, APIs, EVV communications, HHAeXchange integrations, Waystar integrations, and internal administrative interfaces.

Data at Rest

- Production databases
- Backups
- File storage
- Uploaded documents
- Sensitive logs where appropriate
- Developer devices containing company data
- Production infrastructure

Key Management

- Centrally manage keys
- Restrict access
- Never store keys in source code
- Never send secrets through email/chat
- Rotate keys according to documented policy
- Securely back up keys where appropriate

9. Database Security

- Encryption at rest
- Private network access
- No direct public database access
- Firewall/security-group restrictions
- Strong database credentials
- Separate development/staging/production environments
- Database activity logging
- Automated backups
- Point-in-time recovery where supported
- Regular vulnerability assessment
- Restricted administrator privileges

Developers should not routinely access live customer PHI. Where production access is necessary, use time-limited access, approval, MFA, minimum necessary data, and audit logging.

10. Development and Software Security

NexaCareTech will implement a Secure Software Development Lifecycle (SSDLC): Requirements → Design → Development → Testing → Deployment → Monitoring → Retirement.

- Secure coding standards
- Never hard-code credentials
- Never commit secrets to Git
- Approved repositories
- Code review
- Dependency scanning
- Static application security testing where appropriate
- Dynamic/application testing where appropriate
- Secure development environments

Production must be separated from development and staging. Real PHI should not be copied into development environments; use synthetic or de-identified data whenever possible.

11. API Security

- Authentication
- Authorization
- TLS
- Input/output validation
- Rate limiting
- API logging
- Secure error handling
- Token expiration
- Token rotation
- Scope limitations
- Replay protection where appropriate
- Monitoring and abuse detection

API credentials should be unique by environment and integration. HHAeXchange credentials should not be shared with Waystar credentials or development credentials.

12. HHAeXchange and EVV Data Protection

NexaCareTech would establish a dedicated EVV Integration Security Standard covering authentication, API credentials, encryption, data validation, data minimization, transmission logging, error handling, duplicate prevention, authorization, integration monitoring, failed transmission management, data reconciliation, and audit trails.

Every EVV transaction would be traceable: who submitted what, for which client, when, from which system, to which endpoint, what response was received, and the resulting status.

13. Logging and Audit Trails

- Login/logout

- Failed login
- Password reset
- MFA events
- Client record access
- Client record modification
- Record deletion
- Export/download
- Data transmission
- API access
- Administrative changes
- Permission changes
- User creation/deactivation
- Integration activity
- Security events

Audit logs must be protected against unauthorized modification, deletion, excessive access, and premature destruction.

14. Data Minimization

NexaCareTech will collect only information required for a defined business or legal purpose. If a feature does not require a Social Security number, it should not collect one. Data minimization applies to client information, caregiver information, reports, APIs, analytics, logs, support tickets, developer access, and third-party integrations.

15. Data Retention and Destruction

Data	Retention Approach
Client records	Based on customer/legal requirements
EVV records	Customer/regulatory requirements
Billing records	Applicable payer/legal requirements
Audit logs	Security/compliance requirements
Backups	Defined backup lifecycle
Support tickets	Defined business retention
Inactive accounts	Deactivate promptly
Temporary files	Automatic expiration

Each category should have a data owner, purpose, retention period, storage location, legal/customer requirement, and destruction method.

16. Backup and Disaster Recovery

- Automated backups
- Encrypted backups
- Multiple backup copies
- Appropriate geographic/environmental separation
- Restricted backup access
- Backup monitoring
- Backup integrity testing

Recovery Objectives

Define an RPO (Recovery Point Objective) and RTO (Recovery Time Objective) based on customer contracts, technical architecture, and business requirements. Example targets may be RPO ≤ 1 hour and RTO ≤ 4 hours for critical systems, subject to management approval and technical feasibility.

17. Business Continuity

- Cloud outage
- Database failure
- Cyberattack
- Ransomware
- Data corruption
- Major vendor outage
- API/integration failure
- Loss of key personnel
- Natural disaster
- Telecommunications failure

18. Incident Response Plan

Security incidents should follow: Detect → Contain → Investigate → Eradicate → Recover → Notify → Learn.

- Level 1 – Minor: individual failed login attempts
- Level 2 – Significant: compromised account, malware, suspicious API activity
- Level 3 – Critical: unauthorized PHI access, ransomware, production database compromise, large-scale data exfiltration

Every incident must be documented.

19. Breach Response

11. Detection
12. Initial containment
13. Incident commander assignment
14. Evidence preservation
15. Scope determination
16. Determine data affected
17. Determine individuals affected
18. Customer notification
19. Legal review
20. Regulatory notification
21. Individual notification where required
22. Corrective action
23. Post-incident review

We will contractually require vendors to notify NexaCare promptly of suspected or confirmed security incidents, without waiting for a regulatory deadline.

20. Vendor and Third-Party Risk Management

Before Onboarding

- Security controls
- Encryption
- HIPAA status
- SOC 2 report, if available
- Penetration testing
- Incident history
- Data location
- Subprocessors
- Business continuity
- Disaster recovery
- Data retention
- Data deletion
- Access controls
- Insurance
- Contractual protections

Contract Requirements

- Business Associate Agreement where applicable
- Confidentiality
- Security obligations
- Breach notification
- Data-use restrictions
- Subprocessor controls
- Data return
- Data deletion
- Audit rights
- Termination requirements

21. Contractor and Developer Security

- NDA/confidentiality agreement
- Intellectual property agreement
- Security obligations
- Defined system access
- Unique credentials
- MFA
- Least-privilege permissions
- Access expiration

- Secure development environment
- Device security requirements
- No unauthorized downloading of production data

Contractor status must never mean unrestricted access. When a developer leaves: revoke access immediately, rotate credentials where necessary, revoke tokens, review devices/accounts, and review repositories.

22. Employee Security Training

- HIPAA and privacy
- Password security
- MFA
- Phishing and social engineering
- PHI handling
- Secure devices
- Incident reporting
- Data sharing
- Remote work
- Acceptable use

Training should occur before access, at least annually, and after major security changes, significant incidents, new regulatory requirements, or assignment of privileged access.

23. Phishing and Social Engineering

- Phishing
- Business email compromise
- Fake support requests
- Credential theft
- Malicious links
- Fake invoices
- Impersonation
- Password-reset scams

Privileged users should receive enhanced security-awareness training.

24. Mobile and Device Security

- Device encryption
- Screen lock
- Automatic timeout
- Secure application authentication
- MFA where appropriate
- Remote logout/session revocation
- Secure local storage
- No unnecessary PHI storage
- Secure transmission

- Application integrity protections
- Lost/stolen-device procedure

25. Cloud Infrastructure Security

- Network segmentation
- Private subnets where appropriate
- Firewalls/security groups
- Web application firewall
- DDoS protection where appropriate
- Centralized logging
- Security monitoring
- Encryption
- Secrets management
- IAM
- MFA
- Backup
- Vulnerability management
- Configuration monitoring

Development, staging, and production environments should be separated by appropriate cloud accounts or organizational boundaries.

26. Vulnerability Management

- Dependency scanning
- OS patching
- Container scanning if applicable
- Infrastructure scanning
- Application security testing
- API testing
- Cloud configuration review
- Penetration testing

Critical vulnerabilities should receive immediate attention. High-risk vulnerabilities should have defined remediation deadlines. Exceptions must be documented and approved.

27. Penetration Testing

Before broad commercial launch, consider an independent penetration test covering the web application, APIs, authentication, authorization, multi-tenant isolation, mobile application if applicable, cloud configuration, OWASP risks, privilege escalation, data exposure, and session management.

Repeat periodically and after major architectural changes.

28. Multi-Tenant Data Isolation

This is a critical control for NexaCareTech. Agency A must never access Agency B's data.

- Application
- API
- Database
- Storage
- Reporting
- Exports
- Support tools

Security testing should specifically attempt to identify cross-tenant access, broken authorization, insecure direct object references, API manipulation, improper query filtering, and export leakage.

29. Privacy Rights and Customer Requests

- Access requests
- Correction/amendment
- Accounting of disclosures where applicable
- Data export
- Data deletion where legally permissible
- Consent/revocation where applicable
- Privacy complaints

Contracts should clearly establish whether the home-care agency or We are responsible for responding to particular requests.

30. Privacy Policy

We will publish a clear external Privacy Policy explaining what information it collects, why it collects it, how it is used and protected, when it is shared, third-party services, cookies/analytics, retention, security, individual rights, contact information, and policy updates.

The public Privacy Policy does not substitute for contractual privacy/security obligations applicable to customer PHI.

31. Business Associate Agreement Program

- Permitted uses/disclosures
- Safeguards
- Subcontractors
- Incident notification
- Breach notification

- Individual rights support
- Return/destruction of PHI
- Termination
- Regulatory cooperation

The BAA package should be reviewed by healthcare/privacy counsel.

32. Data Processing and Third-Party Disclosure Register

Data	Purpose	System	Recipient	Legal/ Contractual Basis
Client PHI	Care management	NexaCare	Authorized agency users	Customer relationship/BAA
EVV data	EVV processing	NexaCare	EVV partner	Contract/ regulatory
Claims data	Billing	NexaCare	Waystar/payer	Contract/ regulatory
Authentication data	Security	NexaCare	Security systems	Security/ operations
Support information	Support	Support platform	Authorized personnel	Contract/ operations

Maintain a live data map showing data types, purpose, systems, recipients, and legal/contractual basis.

33. Data Flow Mapping

Create diagrams showing: Client → Agency → NexaCare → EVV/HHAeXchange → Billing/Waystar → Payer; and Caregiver → Mobile App → NexaCare API → Database → Agency.

Each flow should identify data type, sender, receiver, encryption, authentication, storage, retention, logging, and legal/contractual basis.

34. Security Governance

- Executive responsibility: CEO / Managing Member
- Security responsibility: Security/Compliance Lead
- Technical responsibility: CTO / Lead Developer
- Privacy responsibility: Privacy/Compliance Officer
- Operational responsibility: Customer/Operations Lead

One person may initially hold multiple responsibilities, but accountability should be explicitly assigned.

35. Risk Register

Risk	Probability	Impact	Mitigation	Owner
Credential theft	High	High	MFA, monitoring	Security
Ransomware	Medium	Critical	EDR, backups	CTO
Cross-tenant	Medium	Critical	RBAC/testing	CTO

access				
API compromise	Medium	High	API security	Developers
Contractor access	Medium	High	Least privilege	CTO
Cloud outage	Medium	High	Disaster recovery	CTO
Data leakage	Medium	Critical	DLP/access controls	Security
Phishing	High	High	Training/MFA	Management
Vendor breach	Medium	High	Vendor assessment	Compliance
Lost device	Medium	High	Encryption/ remote logout	Operations

36. Security Metrics

- MFA adoption
- Critical vulnerabilities outstanding
- High vulnerabilities outstanding
- Security incidents
- PHI incidents
- Failed login attempts
- Unauthorized access attempts
- Employee training completion
- Backup success rate
- Backup recovery test results
- Vendor security reviews completed
- Access reviews completed
- Former-user accounts removed
- Penetration-test findings
- Incident-response exercises completed

37. Quarterly Access Review

At least quarterly, review who has access, what they can access, why they need it, whether access remains necessary, whether former employees/contractors are removed, and whether privileged accounts remain justified.

38. Annual Security Risk Assessment

NexaCareTech will conduct a documented comprehensive risk assessment at least annually and whenever there is a major change in the environment.

- People
- Processes
- Applications
- Databases
- APIs
- Cloud

- Devices
- Vendors
- Integrations
- Physical environment
- Disaster recovery
- Privacy
- Regulatory compliance

39. Incident Exercises

At least annually, NexaCareTech would conduct a tabletop exercise such as: an attacker obtains administrator credentials and accesses the production environment.

- Who detects it?
- Who is notified?
- Who shuts down access?
- Who investigates?
- Who contacts the customer?
- Who determines whether PHI was accessed?
- Who contacts legal counsel?
- Who handles regulatory notification?
- How is the system restored?
- What changes afterward?

A second exercise should simulate ransomware or a major cloud outage.

40. Customer Security Assurance

NexaCareTech will maintain a Customer Security & Privacy Overview that can be shared during sales and due diligence.

- HIPAA program
- Encryption
- MFA
- Access control
- Audit logging
- Backup
- Disaster recovery
- Incident response
- Vendor management
- Security testing
- Data retention
- Privacy Policy
- BAA process
- Security contact

Rather than simply stating 'Your data is secure,' We will demonstrate how the platform protects data.

41. NexaCareTech Data Protection & Privacy Commitment

NexaCareTech Commitment to Protecting Your Data

At NexaCareTech, protecting the information entrusted to us is fundamental to how we build and operate our platform.

We are designed with privacy and security at its core. We use layered administrative, technical, and physical safeguards to protect sensitive information, including protected health information, against unauthorized access, use, disclosure, alteration, loss, or destruction.

Our approach includes role-based access controls, multi-factor authentication, encryption, secure software development, audit logging, controlled third-party integrations, regular security assessments, secure backups, incident-response procedures, and ongoing monitoring.

We follow the principle of least privilege: users and systems receive only the access necessary to perform their authorized functions. We also apply data-minimization principles and work to ensure that sensitive information is collected, used, transmitted, and retained only for legitimate and authorized purposes.

We maintain documented policies governing privacy, information security, access management, incident response, data retention, vendor management, and business continuity. Our employees, developers, contractors, and service providers are required to follow applicable security and confidentiality requirements.

For healthcare organizations, we support appropriate contractual and compliance requirements, including Business Associate Agreements where applicable.

Our commitment is simple: Your data deserves the highest level of care, protection, and accountability.

NexaCareTech — secure technology for better care.

---

42. Recommended NexaCare Security Architecture

Users → MFA + Secure Authentication → Web/Mobile Application → API Gateway / WAF → Authorization + Tenant Isolation → Application Services → Encrypted Database / Secure File Storage → Encrypted Backups.

Controlled integrations should connect to HHAeXchange / EVV, Waystar / Billing, and other approved healthcare partners, with centralized logging and security monitoring across the environment.

43. Ten Non-Negotiable Security Rules

24. No unauthorized person may access customer PHI.
25. No employee or developer receives more access than necessary.
26. No production PHI is used in development or testing unless specifically authorized and appropriately protected.
27. All privileged accounts require MFA.
28. All sensitive data must be encrypted in transit and at rest where technically appropriate.
29. Passwords and API secrets may never be stored in source code.
30. Every access to sensitive production systems must be attributable to a specific person or service identity.
31. Every suspected security incident must be reported immediately.
32. Third parties cannot receive NexaCare customer data without an approved business and security basis.
33. Security is a product requirement—not an optional feature.

Review and Version History

This Framework is adopted by NexaCareTech LLC with effect from the date stated above. It shall be reviewed at least annually, and in any event upon a material change to the Company's systems, processing activities, vendor arrangements or regulatory obligations.

Any amendment to this Framework shall be recorded in the version history below. Material amendments shall be notified to all persons to whom this Framework applies.

Version	Date	Summary of change	Issued by
1.0	October 2026	Initial issue	NexaCareTech LLC
1.1	4 October 2026	Document control, status and approval provisions added; launch readiness and roadmap separated into their own document; content otherwise unchanged	NexaCareTech LLC