Information Security & Safeguards Overview

Heka Intelligence • Version 1.0 • April 29, 2026

Purpose. This document describes the administrative, technical, and organizational safeguards Heka Intelligence applies to clinic and patient health information. It is intended to support clinic security reviews, vendor risk assessments, and Alberta *Health Information Act* (HIA) Privacy Impact Assessment submissions to the Office of the Information and Privacy Commissioner of Alberta (OIPC).

1. Security program overview

Heka Intelligence operates a healthcare workflow platform for Canadian clinics, with a focus on Alberta family medicine. Heka's security program is designed around the principles in Alberta's Health Information Act, the Health Information Regulation, the Personal Information Protection Act (PIPA), and the Personal Information Protection and Electronic Documents Act (PIPEDA), as well as widely-recognized security frameworks (ISO/IEC 27001 and NIST CSF) used as design references.

Security is overseen by Heka's Privacy Officer, who is responsible for the privacy program, vendor reviews, breach response, and the maintenance of this document.

Defense-in-depth model

Heka layers safeguards across four control families:

- **Administrative —** policies, training, access reviews, vendor risk management, contracts.
- **Technical —** encryption, authentication, access controls, network segmentation, logging, monitoring.
- **Physical —** inherited from Canadian-region cloud providers operating audited data centres.
- **Organizational —** personnel screening, confidentiality obligations, role-based duties, incident response governance.

2. Hosting and data residency

Heka production workloads are hosted on Amazon Web Services (AWS) Canadian regions (primary: ca-west-1, Calgary). For Alberta clinic deployments, identifiable health information is stored and processed on Canadian infrastructure by default.

Production environment

- **Compute:** AWS Lambda, ECS, and EC2 within Canadian regions; no production identifiable PHI on developer workstations.
- **Storage:** AWS S3 (server-side encrypted, KMS-managed keys) and DynamoDB (encryption at rest enabled by default) for structured records and document blobs.
- **Messaging:** AWS SQS for asynchronous workflow events, encrypted in transit and at rest.
- **Networking:** Private VPCs, security groups enforcing least-privilege traffic, no direct public ingress to data stores, TLS-terminated edge.

Cross-border processing

Where a specific feature requires processing outside Canada (for example, a third-party model provider), Heka:

- discloses the cross-border processing in the Subprocessor List;
- contractually restricts the provider from using clinic data for unrelated purposes or model training;
- limits the information sent to what is strictly necessary for the workflow; and
- offers Alberta clinics the option to disable features that involve cross-border processing.

3. Encryption

Encryption in transit

- All external endpoints terminate TLS 1.2 or higher; HSTS is enforced on web endpoints.
- Internal service-to-service traffic uses TLS or runs over private VPC networks.
- Inbound fax ingestion partners deliver content over authenticated, encrypted channels.

Encryption at rest

- Object storage (S3) encrypted with AWS KMS using AES-256.
- Database stores (DynamoDB, RDS where used) encrypted with AWS KMS at the storage layer.
- Backups and snapshots encrypted using the same KMS hierarchy.
- Application-level field encryption is applied to selected sensitive fields where the threat model warrants additional protection beyond storage-layer encryption.

Key management

Encryption keys are managed in AWS KMS. Key access is restricted via IAM policy, separated from data-plane access, and rotated according to AWS-managed key rotation policies (or shorter, where required by clinic contract).

4. Identity, authentication, and access control

User authentication

- Strong password requirements aligned with NIST SP 800-63B guidelines.
- Multi-factor authentication (MFA) required for administrative roles and recommended/enforced for clinical users based on clinic configuration.
- Session timeout, idle lockout, and re-authentication for sensitive actions.

Authorization model

Heka implements role-based access control (RBAC) with clinic-configurable roles. Common role classes include:

- **Clinic Administrator —** user management, workflow configuration, audit log review.
- **Provider —** patient records, referrals, clinical context relevant to assigned panel.
- **Clinic Staff / MOA —** referral processing, fax handling, patient communication, scheduling.
- **Read-only / Reviewer —** audit, reporting, no write capability.

Permissions follow the principle of least privilege. Clinics configure which users access which workflows, queues, documents, and administrative functions.

Heka personnel access

- Production access is limited to a small number of authorized personnel with a documented operational need.
- Personnel access is logged, time-bound where feasible, and subject to periodic access reviews.
- Privileged operations require MFA and are logged to immutable audit storage.
- All Heka personnel sign confidentiality agreements covering clinic and patient information and are subject to internal policy on access to personal and health information.

5. Logging, monitoring, and audit

Audit logging

Heka generates audit log entries for sensitive activity, including:

- login, logout, and authentication failure events;
- administrative actions (role changes, workflow configuration changes, integration toggles);

- document handling events (view, download, route, classify, redact);
- referral lifecycle events (create, send, status change, decline, close);
- AI-assisted action events (suggestion generated, accepted, rejected, modified);
- data export and deletion events; and
- security-relevant events (privilege escalation, anomalous access patterns).

Monitoring

- Centralized log aggregation with retention aligned to operational and contractual requirements.
- Alerting on authentication anomalies, infrastructure errors, integration failures, and suspicious access patterns.
- Application performance and availability monitoring with on-call rotation.

Audit support to clinics

On request, Heka can provide clinic administrators with access to audit information relevant to their tenant for the purpose of internal review, regulatory inquiry, or breach investigation, subject to applicable contractual terms.

6. Network and infrastructure security

- Production environments are segmented from non-production (development, staging) environments. No identifiable PHI is permitted in non-production environments — synthetic or de-identified data is used for development and testing.
- Public-facing services sit behind a managed edge layer with rate limiting, web application firewall protections, and DDoS mitigation provided by the cloud platform.
- Internal services communicate over private VPC networks; databases are not exposed to the public internet.
- Infrastructure is defined as code; changes are reviewed via pull request, tested in non-production, and deployed through controlled CI/CD pipelines.

7. Application and AI security

Secure software development

- Source control hosted on a tier-one platform with branch protection and required review on the main branch.
- Dependency scanning, secret scanning, and static analysis run on pull requests.
- Vulnerabilities are tracked, prioritized by severity, and remediated within target windows that depend on severity.
- Secrets are stored in a managed secret store (e.g., AWS Secrets Manager, SSM Parameter Store) and are not committed to source control.

AI workflow safeguards

Heka uses AI to assist with administrative workflows (document classification, referral status extraction, draft communication generation, queue prioritization). AI safeguards include:

- **Private hosting —** AI processing for clinic workflows runs on Heka-controlled infrastructure or on contracted providers under enterprise terms; clinic data is not sent to public consumer AI tools.
- **No public model training —** Heka does not use identifiable clinic or patient information to train public AI models, and contractually prohibits providers from doing so.
- **Minimum-necessary input —** AI workflows receive only the data required for the specific task.
- **Human-in-the-loop —** AI outputs are reviewed by authorized clinic staff for sensitive actions; clinics configure which actions require explicit review.
- **Auditability —** AI-assisted events are logged with the source artifact, suggestion, reviewer, and outcome where technically feasible.
- **Prompt and output safety —** system prompts and tool definitions are version-controlled and reviewed; output classes that could affect patient communication are gated by review.

8. Backups, business continuity, and disaster recovery

- Automated backups of production data stores with encryption preserved end-to-end.
- Backup restoration is tested on a defined cadence to verify recoverability.
- Recovery objectives — Recovery Time Objective (RTO) and Recovery Point Objective (RPO) — are documented and reviewed annually.
- Region-redundant storage where supported by the underlying cloud service.
- Operational runbooks cover degraded-service scenarios (e.g., upstream provider outage, fax ingestion failure, AI provider outage) and define manual fallback procedures so clinics can continue core referral operations.

9. Vendor and subprocessor management

- Heka maintains a Subprocessor List (companion document) identifying third-party service providers that may process clinic or patient information.
- New subprocessors are reviewed for security posture, data residency, contractual protections, and necessity before adoption.
- All subprocessors are bound by written agreements requiring confidentiality, security safeguards, restricted use, and breach notification.
- Material changes to the subprocessor list will be communicated to clinics consistent with contractual notice obligations.

10. Incident response and breach notification

Detection and response

Heka maintains a documented incident response process with the following phases: detection, triage and classification, containment, eradication, recovery, and post-incident review. The Privacy Officer is the accountable owner; an on-call engineer leads technical response.

Notification

If Heka becomes aware of unauthorized access, use, disclosure, loss, or compromise of clinic or patient information, Heka will:

- notify the affected clinic without undue delay and in accordance with contractual timelines;
- provide the clinic with information reasonably required to assess severity, scope, and risk of harm — including data categories involved, individuals potentially affected, root cause (where known), and remediation steps;
- cooperate with the clinic's own notification obligations to the OIPC and affected individuals under the HIA, and to the federal Privacy Commissioner under PIPEDA's breach-of-security-safeguards requirements where applicable; and
- conduct a documented post-incident review and implement corrective actions.

Records

Heka maintains records of privacy and security incidents, including those that did not require notification, consistent with PIPEDA s.10.3 record-keeping obligations and contractual commitments.

11. Personnel safeguards

- Background checks for personnel with access to production systems, where permitted by law and proportional to role sensitivity.
- Confidentiality agreements covering personal information and health information signed at hiring and reaffirmed periodically.
- Security and privacy training at onboarding and annually thereafter, including HIA, PIPEDA, and AI use awareness.
- Role-based duty separation: developers do not have standing access to production identifiable data; production access is granted just-in-time for documented operational reasons.
- Defined offboarding process that revokes access, recovers credentials and devices, and confirms access removal across systems.

12. Physical security

Heka does not operate its own data centres. Physical safeguards for production data are inherited from the underlying cloud provider's audited Canadian-region facilities, which are subject to industry attestations (e.g., ISO 27001, SOC 2, CSA STAR).

Heka office and remote-work environments are governed by a clean-desk and device security policy: full-disk encryption, screen lock, remote-wipe capability for managed devices, and prohibition on storing identifiable PHI on local workstations.

13. Compliance and assurance

Heka's security program is designed to support compliance with the legal and contractual frameworks below. Heka does not assert formal certification under each framework unless explicitly noted; references indicate the design intent of the program.

Framework	Role in Heka's program
Alberta Health Information Act (HIA)	Primary statute governing patient health information for Alberta clinics; Heka acts as Information Manager under s.66 HIR.
Alberta Health Information Regulation	Defines required terms for custodian–information manager agreements; Heka's contracts are designed to align.
PIPEDA	Federal private-sector privacy law; informs Heka's accountability, consent, safeguards, breach-of-safeguards, and record-keeping obligations.
Alberta PIPA	Alberta private-sector privacy law; informs Heka's handling of non-health personal information.
ISO/IEC 27001 (design reference)	Used as a design reference for the information security management system.
NIST CSF (design reference)	Used as a design reference for risk management, detection, response, and recovery functions.

14. Document maintenance

This document is reviewed at least annually and on material change to the platform architecture, subprocessors, or applicable law. The current version is available from the Privacy Officer.

> **Contact — Privacy Officer**
> Heka Intelligence
> Email: deep@hekaintelligence.com