Privacy Policy

Heka Intelligence • Last updated: April 29, 2026

> This Privacy Policy explains how **Heka Intelligence** ("Heka," "we," "us," or "our") collects, uses, discloses, stores, protects, retains, and deletes information when clinics, physicians, clinic staff, patients, caregivers, and authorized users interact with Heka's referral, fax, document, and care-coordination workflows. Heka is designed for Canadian healthcare environments — including Alberta family medicine clinics — and is built around privacy, security, confidentiality, Canadian data residency, clinic control, auditability, and responsible AI use.

We do not sell patient information. We do not use patient information for advertising. We do not train public AI models on clinic or patient information.

Heka processes health information only to provide services to the clinic, support clinic-approved workflows, protect security, comply with law, and improve the reliability, safety, and performance of the Heka platform.

1. Scope of this Privacy Policy

This Privacy Policy explains how Heka collects, uses, discloses, stores, protects, retains, and deletes personal information and health information when clinics, physicians, clinic staff, patients, caregivers, and authorized users interact with Heka's products and services.

This Privacy Policy applies to Heka's clinic-facing platform; referral management tools; inbound fax and document workflows; AI-assisted document classification and routing; patient communication workflows; patient-facing referral updates where enabled; appointment, follow-up, and reminder workflows; staff queues and clinic dashboards; integrations with clinic systems, including EMRs where enabled; Heka support services; Heka websites; and any other services that link to this Privacy Policy.

Heka is an operational workflow platform. Heka does not replace the clinic, physician, regulated health professional, EMR, or clinical judgment. The clinic remains responsible for patient care, clinical decision-making, medical records, and determining how patient information is used in the provision of care.

2. Heka's role under Alberta healthcare privacy law

In Alberta, family physicians and clinics are generally responsible for patient health information under Alberta's **Health Information Act** (the "HIA"). The HIA governs health information in the custody or under the control of a custodian, including rules for collection, use, disclosure, access, and protection of health information.

For most clinic deployments, the clinic, physician, or applicable healthcare organization is the **custodian** of patient health information. Heka acts as a technology service provider and, where applicable, an **information manager** that processes, stores, retrieves, transforms, or manages health information on behalf of the clinic.

Under Alberta's **Health Information Regulation**, an agreement between a custodian and an information manager must address the information management services being provided and related safeguards and obligations. Heka therefore expects to enter into appropriate contractual terms with Alberta clinics, which may include an Information Manager Agreement, privacy and security obligations, confidentiality obligations, permitted-use restrictions, breach notification obligations, subcontractor controls, audit support, and return or deletion obligations.

Heka processes clinic and patient information only on behalf of the clinic and only for the purposes described in this Privacy Policy, the clinic's agreement with Heka, and the clinic's configuration of the Heka platform.

3. Legal and privacy standards Heka is designed to support

Heka is designed to support compliance with applicable Canadian and Alberta healthcare privacy standards, including the following.

Alberta Health Information Act

The HIA governs the collection, use, disclosure, and protection of health information by custodians in Alberta healthcare settings. The Office of the Information and Privacy Commissioner of Alberta oversees compliance with the HIA by custodians and affiliates.

Heka supports clinic compliance with the HIA through role-based access controls, least-privilege permissions, audit logs, clinic-configurable workflows, Canadian data residency, secure hosting, encryption, access controls, breach response processes, and contractual information-manager obligations.

Alberta Health Information Regulation

The Health Information Regulation includes requirements for agreements between custodians and information managers. Heka's contractual model is designed to align with these requirements by defining the services provided, the permitted purposes of processing, safeguards, access restrictions,

confidentiality requirements, subcontractor controls, and obligations in the event of unauthorized access, use, disclosure, loss, or compromise.

Privacy Impact Assessment support

Under section 64 of Alberta's HIA, custodians must submit Privacy Impact Assessments to the Commissioner for review and comment before implementing administrative practices or information systems — or changes to such practices or systems — that collect, use, or disclose individually identifying health information.

Heka supports clinics with documentation needed for a Privacy Impact Assessment, including product architecture summaries, workflow descriptions, data flow descriptions, data residency details, access control descriptions, security safeguards, AI workflow explanations, subprocessors, retention logic, breach response procedures, and auditability controls.

Heka does not replace the clinic's responsibility to determine whether a Privacy Impact Assessment is required or to submit one to the Alberta OIPC unless separately agreed.

PIPEDA and Alberta private-sector privacy principles

PIPEDA applies to private-sector organizations in Canada that collect, use, or disclose personal information in the course of commercial activity, and it is built around fair information principles such as accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, safeguards, openness, individual access, and challenging compliance.

Alberta also has the **Personal Information Protection Act** (PIPA), which is Alberta's private-sector privacy law for provincially regulated private-sector organizations.

While patient health information in Alberta clinics is primarily governed by the HIA, Heka's broader privacy program is designed around Canadian privacy principles, including accountability, limited collection, clear purposes, appropriate consent where required, limited use and disclosure, safeguards, transparency, access, correction, breach response, and retention limitation.

4. Information Heka collects and processes

The information Heka processes depends on the clinic's configuration, integrations, workflows, and instructions.

A) Clinic and user account information

Heka may collect and process information about clinics and authorized users, including:

- clinic name; clinic contact details; physician and provider names; staff names; user emails; user roles; permissions; login credentials or authentication metadata;
- clinic locations; operating hours; provider schedules; referral workflows; specialty routing preferences; communication templates; escalation rules; and support communications.

B) Patient and health information

Where enabled by the clinic, Heka may process patient information and health information, including:

- patient name; date of birth; phone number; email address; health card or clinic identifier where required; family physician or provider;
- referral reason; specialty requested; clinical context relevant to the referral; referral documents; consult letters; inbound faxes;
- appointment details; patient communication history; referral status; specialist office responses; decline reasons; follow-up requirements; and task notes entered by clinic staff.

Heka is designed to process only the **minimum information** required to complete the clinic-approved workflow.

C) Communications and documents

Where enabled, Heka may process:

- inbound faxes; outbound referral packages; consult letters; patient forms; clinic notes provided to Heka;
- phone call metadata; call transcripts where enabled; voicemail content where enabled; SMS or email content where enabled;
- appointment reminders; referral status messages; patient follow-up messages; and staff communications within the platform.

D) EMR and integration data

Where a clinic enables an integration, Heka may receive or send limited data to authorized systems, including EMRs, fax providers, scheduling systems, secure messaging systems, patient communication tools, or other clinic-approved systems.

Heka's integration design follows a **minimum-necessary** approach. For example, Heka may use integration data to match an inbound fax to a patient, update a referral status, create a staff task, surface an overdue referral, generate a draft communication, or send a clinic-approved update.

E) Technical and security information

Heka may collect technical and security information needed to operate and protect the platform, including:

- IP address; device and browser metadata; login events; access timestamps; authentication events;
- role and permission changes; API events; system logs; audit logs; error logs; performance telemetry; security alerts; and infrastructure monitoring data.

5. How Heka uses information

Heka uses information only for legitimate clinic, operational, security, legal, and product reliability purposes. Heka may use information to:

- provide, operate, maintain, and secure the Heka platform;
- support referral management and closed-loop referral workflows;
- process inbound faxes and clinical documents;
- classify and route documents to clinic staff;
- create staff tasks and work queues;
- support patient communication, appointment, reminder, and follow-up workflows approved by the clinic;
- match documents to patients where instructed by the clinic;
- summarize workflow-relevant information for staff review;
- integrate with clinic systems as configured by the clinic;
- authenticate users and administer clinic accounts;
- monitor reliability, uptime, and platform performance;
- investigate bugs, errors, and support issues;
- detect, prevent, and respond to security incidents or misuse;
- maintain audit logs and workflow evidence trails;
- comply with legal and contractual obligations; and
- improve the safety, reliability, usability, and accuracy of the Heka platform.

Heka does not use patient information for unrelated business purposes; sell patient information; use patient information for advertising, ad targeting, or marketing profiles; use identifiable patient information to train public AI models; disclose patient information to third parties for their independent commercial use; or use patient information to make automated clinical decisions.

6. AI processing and responsible AI safeguards

Heka uses AI to support administrative and operational workflows — not to replace clinical judgment. AI may be used to assist with:

- inbound fax classification; document routing; referral status extraction; referral package organization;
- specialist response categorization; consult letter identification; patient communication drafting;
- task prioritization; workflow summarization; duplicate detection; missing-information checks; and staff queue generation.

Heka's AI workflows are designed around the following safeguards:

Private AI processing

Heka's AI processing for clinic workflows is privately hosted and controlled. Clinic and patient information is not sent to public consumer AI tools.

Canadian hosting

Where configured and contracted, Heka stores and processes production clinic and patient data on Canadian servers. Heka's architecture is designed to support Canadian data residency for Alberta clinic deployments.

No public model training

Heka does not use identifiable clinic or patient information to train public AI models. Heka does not allow third-party AI model providers to use clinic or patient data for their own model training.

Human-in-the-loop review

Heka's AI outputs are designed to assist clinic staff. They should be reviewed by authorized clinic users where appropriate, especially for sensitive workflows, referral decisions, patient communications, document routing, and clinical context.

Minimum necessary context

AI workflows are designed to access only the data needed for the specific task. For example, an AI classifier may need the document type and relevant text from a fax, but not unrelated patient records.

Auditability

Heka maintains logs of relevant AI-assisted workflow events, including the source document, suggested classification or routing, user review, workflow action, and outcome where technically feasible.

Clinic configuration

Clinics can configure which AI workflows are enabled, what information is available to those workflows, what actions require staff review, and which users can approve or modify AI-assisted outputs.

7. Data residency and hosting

Heka is designed for Canadian healthcare use and supports **Canadian data residency**.

Where configured and contracted, Heka stores and processes clinic and patient information on servers located in Canada. Heka's default position for Alberta clinic deployments is that identifiable health information should remain in Canada unless the clinic expressly approves otherwise and appropriate contractual, technical, and legal safeguards are in place.

If a specific feature, support activity, integration, or service provider requires cross-border processing, Heka will:

- notify or disclose the processing to the clinic where required;
- limit the information involved to what is necessary;
- use contractual restrictions;
- require confidentiality and security safeguards;
- restrict the provider from using the information for unrelated purposes; and
- comply with applicable law and clinic contractual requirements.

8. Security safeguards

Heka uses administrative, technical, and organizational safeguards appropriate to the sensitivity of healthcare information.

Encryption

- **In transit:** Heka uses encryption in transit to protect data transmitted between users, clinics, integrations, and Heka systems.
- **At rest:** Heka uses encryption at rest for stored data, including databases, documents, files, transcripts, logs, and backups where applicable.

Access controls

Heka uses **role-based access control (RBAC)**, least-privilege access, strong authentication, administrative access controls, and permission management. Clinic administrators can configure which users have access to specific workflows, patient records, referral queues, documents, and administrative functions.

Audit logging

Heka maintains audit logs for sensitive activity, including login events, user access, administrative actions, document handling, referral status changes, AI-assisted actions, integration activity, exports, and security-relevant events where technically feasible.

Segregation and confidentiality

Heka is designed to separate clinic environments and restrict access to clinic data to authorized users, services, and support personnel with a legitimate need. Heka personnel are subject to confidentiality obligations and internal policies governing access to personal information and health information.

Secure development and operations

Heka uses secure development and operational practices, including access reviews, security monitoring, vulnerability remediation, secure configuration management, production access controls, backup procedures, incident response processes, and logging of security-relevant events.

Backups and availability

Heka uses backup and recovery practices designed to support business continuity and reduce the risk of data loss. Backup access is restricted and protected by appropriate safeguards.

Incident response

Heka maintains processes to detect, contain, investigate, remediate, and document privacy and security incidents. If Heka becomes aware of unauthorized access, use, disclosure, loss, or compromise of clinic or patient information, Heka will notify the affected clinic as required by law and contract and will provide information reasonably necessary for the clinic to assess and meet its own legal obligations.

PIPEDA includes breach-of-security-safeguards obligations, including reporting to the federal Privacy Commissioner and notifying affected individuals where a breach creates a real risk of significant harm.

9. Clinic control and configuration

Heka is designed so clinics remain in control of their workflows and patient information. Clinics can configure:

- enabled workflows; staff roles and permissions; referral categories; routing rules; document classification rules; escalation paths;
- patient communication templates; patient communication channels; AI-assisted workflows; human review requirements;
- EMR or system integrations; retention settings where available; and user access levels.

Clinics are responsible for determining how Heka should be configured for their practice, legal obligations, professional obligations, consent model, patient communication practices, and internal privacy program.

10. Disclosure of information

Heka discloses information only as needed to provide the services, follow clinic instructions, protect security, comply with law, or fulfill contractual obligations.

A) Disclosure to the clinic

Heka shares information with the clinic and authorized clinic users so they can manage referrals, respond to patients, review documents, complete tasks, follow up on care gaps, and provide care.

B) Disclosure to service providers

Heka may use service providers to support hosting, infrastructure, secure communications, logging, monitoring, support, analytics, security, and related operations. Service providers are required to protect information, maintain confidentiality, use information only to provide services to Heka, and comply with contractual privacy and security obligations.

C) Disclosure to clinic-approved integrations

Where enabled by the clinic, Heka may exchange information with authorized systems such as the clinic's EMR, fax provider, scheduling system, secure messaging platform, patient communication tool, or specialist network.

D) Legal and safety disclosures

Heka may disclose information where required by law, regulation, court order, legal process, regulator request, professional obligation, or where necessary to protect the rights, safety, or security of Heka, clinics, patients, users, or others.

E) Business transfers

If Heka is involved in a merger, acquisition, financing, reorganization, sale of assets, or similar transaction, information may be transferred as part of that transaction, subject to appropriate confidentiality, security, and legal protections.

11. Retention, deletion, and export

Heka retains information only as long as necessary to provide the services, support clinic workflows, comply with legal obligations, maintain auditability, resolve disputes, enforce agreements, and protect security. Retention periods may depend on:

- clinic configuration; clinic contract terms; applicable legal and regulatory requirements;
- clinical recordkeeping requirements; audit requirements; security requirements; operational support needs; and backup cycles.

Clinics may request export, return, or deletion of certain data, subject to applicable law, contractual terms, technical limitations, and the clinic's own recordkeeping obligations.

Because clinics are generally the custodians of patient health information, patients should usually contact their clinic directly for access, correction, deletion, or record-related requests.

12. Patient rights and requests

Patients may have rights to request access to or correction of their health information under applicable law. Alberta's HIA gives individuals rights relating to health information in the custody or under the control of custodians.

Because Heka usually processes information on behalf of a clinic, patients should contact their clinic first for requests involving:

- medical records; referral records; appointment information; clinical notes; consult letters;
- correction requests; access requests; disclosure questions; questions about care; and questions about clinic-controlled patient information.

If Heka receives a patient request directly, Heka may redirect the patient to the clinic or coordinate with the clinic as appropriate.

13. Consent and patient communications

In healthcare settings, the clinic determines the appropriate legal authority, consent model, and patient communication process for collecting, using, and disclosing patient information.

Where Heka communicates with patients on behalf of a clinic, Heka does so according to the clinic's instructions and configuration. Patient communications may include:

- appointment reminders; referral status updates; missing-information requests; follow-up reminders;
- scheduling coordination; inbound message responses; care coordination updates; and clinic-approved administrative communications.

Patients may be able to opt out of certain non-essential communications depending on clinic configuration and legal requirements. Opting out may affect the clinic's ability to provide automated reminders or updates.

Heka supports clinics by providing clear workflow configuration, patient-facing messaging where enabled, and documentation about how information is processed.

14. Privacy Impact Assessment and clinic onboarding support

For Alberta clinics, Heka can provide materials to support the clinic's Privacy Impact Assessment process. These materials may include:

- product overview; workflow descriptions; data flow diagrams; types of information collected; purposes of use;
- access control model; role and permission structure; data residency description; hosting environment description;
- security controls; encryption overview; audit logging description; AI workflow description;
- subprocessor list; breach response process; backup and retention approach; and data export/deletion process.

Heka does not submit the clinic's Privacy Impact Assessment on behalf of the custodian unless separately agreed. The clinic remains responsible for determining whether a Privacy Impact Assessment is required and submitting it to the OIPC where required.

15. Website privacy, cookies, and analytics

Heka's public website may use cookies, analytics tools, and similar technologies to provide website functionality, understand site usage, improve performance, and protect the website.

Website analytics are separate from production clinic health information. Heka does not use patient health information from clinic workflows for advertising or website retargeting. Users can manage cookies through browser settings.

16. Children and minors

Heka may process information about minors where a clinic uses Heka in connection with family medicine, pediatric, or dependent care workflows.

Heka does not knowingly collect information directly from children outside of clinic-directed workflows. Where information about a minor is processed, it is processed on behalf of the clinic and subject to the clinic's instructions and applicable law.

Parents, guardians, and substitute decision-makers should contact the clinic directly for questions about a minor's care or records.

17. Changes to this Privacy Policy

Heka may update this Privacy Policy from time to time. When we update this Privacy Policy, we will revise the "Last updated" date. Where changes materially affect how Heka handles clinic or patient information, Heka will provide notice as required by law or contract.

18. Contact

For privacy questions, security questions, or requests, contact:

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

Patients should also contact their clinic directly for questions about care, referral status, appointment information, medical records, or clinical decision-making.