

Specimen — illustrative example

Northvale Health Analytics is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Privacy and Personal Information Policy

Northvale Health Analytics

Document type	policy	Version	1.0 Draft
Owner	Chief Technology Officer	Customer decision role	Chief Executive Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Northvale Health Analytics	Industry	Health technology
Organization size	26-100	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

Northvale Health Analytics operates at the intersection of clinical care and technology. The personal information it handles — including patient referral content and clinician account data

— is among the most sensitive information any organisation can hold. A breach of that information can harm patients, damage the trust of referring practices, and expose Northvale to regulatory and legal consequences.

This policy states Northvale's commitment to handling personal information lawfully, transparently and with care proportionate to its sensitivity. It sets out who is accountable, what is required at each stage of the information lifecycle, and how Northvale meets its obligations to the individuals whose information it holds and to the practices that entrust it with that information.

2. Scope

This policy applies to:

- (a) all personal information collected, received, stored, used, disclosed or disposed of by Northvale Health Analytics in the course of its operations;
- (b) all employees, contractors, secondees and any other individuals who access or handle personal information on Northvale's behalf;
- (c) all systems, platforms and services used to process personal information, including the Northvale platform hosted in Azure Canada Central and the managed laptops through which clinicians access it.

This policy covers two principal categories of personal information:

— Patient information: names, health card numbers, presenting complaints and clinical histories contained in referral letters received from Ontario family physicians.

— Clinician information: account and identity data for the clinicians who use the Northvale platform.

Internal operational metrics that do not identify individuals fall outside this policy's scope. Where they are combined with identifiable information, the combined dataset is in scope.

3. Definitions

Personal information means any information about an identifiable individual. In Northvale's context this includes, but is not limited to, a patient's name, health card number, presenting complaint and clinical history, and a clinician's name and account credentials.

Processing means any operation performed on personal information, including collection, receipt, storage, use, disclosure, transfer, retention and disposal.

Consent means a freely given, specific, informed and unambiguous indication by a data subject that they agree to the processing of their personal information for a stated purpose. Consent may be express or, where applicable law permits, implied.

Data subject means the identified or identifiable individual to whom personal information relates. In Northvale's operations, data subjects are primarily patients named in referrals and clinicians who hold platform accounts.

Privacy incident means any event — confirmed or suspected — that involves unauthorised access to, collection, use, disclosure, retention or disposal of personal information, or any failure of a control that protects personal information. This includes breaches by Northvale staff, by suppliers, and by technical failure.

4. Accountability

4.1 Policy owner

The Chief Technology Officer owns this policy. The Chief Technology Officer is accountable for maintaining it, ensuring it is implemented, and reporting on its effectiveness to the Chief Executive Officer.

4.2 Executive accountability

The Chief Executive Officer holds ultimate accountability for Northvale's privacy obligations. The Chief Executive Officer reviews and records their review of this policy on the annual cycle set out in Section 12.

4.3 All staff

Every employee and contractor who handles personal information is personally responsible for complying with this policy. Compliance is a condition of engagement. Failure to comply may result in disciplinary action up to and including termination.

4.4 Relationship to other instruments

This policy operates alongside the Information Security Policy, the Data Classification and Handling Standard, the Third-Party Risk Management Policy, the Privacy Breach Response Procedure, and the Records Retention and Disposal Policy. Where those instruments set more

specific requirements for a topic this policy also covers, both apply. This policy does not duplicate what those instruments already own.

5. Lawful Authority, Purpose and Transparency

5.1 Lawful authority

Northvale must identify a lawful basis for processing before any processing begins. Northvale processes patient referral content as a service provider to the referring practice under a written agreement. The referring practice is the custodian of that information under applicable Ontario privacy law; Northvale acts on the practice's authority and within the limits of that agreement. Northvale does not rely on patient consent as its own independent basis for processing referral content.

For clinician account data, the lawful basis is the contractual relationship between Northvale and the clinician or their employing organisation.

5.2 Purpose limitation

Northvale processes personal information only for the purpose of routing and prioritising care referrals on behalf of referring practices. No secondary use is permitted. Personal information must not be used for marketing, product development, model training, research or any other purpose not stated in the written agreement with the referring practice.

Any proposed new processing purpose must be assessed under Section 6 before it begins. The Chief Technology Officer must record that assessment.

5.3 Transparency

Northvale must maintain a record of its processing activities. That record must state, for each processing activity: the category of personal information involved, the purpose, the lawful basis, the retention period, and the parties with whom information is shared. The Chief Technology Officer is responsible for keeping this record current.

Northvale must be able to describe its processing activities to referring practices on request. Northvale does not communicate directly with patients about its processing role; that responsibility rests with the referring practice as custodian.

6. Privacy Assessment Before Processing

6.1 When an assessment is required

A privacy assessment must be completed before Northvale:

- (a) begins processing a new category of personal information;
- (b) introduces a new processing purpose;
- (c) onboards a supplier that will process personal information (see also Section 10);
- (d) makes a material change to a system or process that handles personal information;
- (e) transfers personal information to a new jurisdiction or storage location.

6.2 What the assessment must cover

The assessment must identify: the personal information involved and its sensitivity; the purpose and lawful basis; the risks to data subjects if the information is lost, misused or disclosed without authority; the controls that will mitigate those risks; and any residual risk that requires a decision by the Chief Technology Officer or Chief Executive Officer.

6.3 Record and review

The Chief Technology Officer must retain each completed assessment. Assessments for active processing activities must be reviewed on the annual cycle set out in Section 12, or sooner if a material change occurs.

7. Data Minimisation and Use Limitation

7.1 Collect only what is necessary

Northvale must collect and receive only the personal information that is reasonably necessary to route and prioritise the referral. Staff must not request, store or retain information beyond what the agreed purpose requires.

7.2 No secondary use

Personal information received from referring practices must not be used for any purpose other than the one stated in the written agreement. This prohibition applies to all staff and to all suppliers acting on Northvale's behalf.

7.3 No training use

Patient referral content and clinician account data must not be used to train, fine-tune or evaluate any machine learning or AI model, whether operated by Northvale or by a supplier. This requirement must be reflected in every supplier agreement that involves access to personal information. Alignment with the AI Acceptable Use Policy and the AI Risk Management Standard is required where AI systems interact with personal information.

7.4 Aggregation and de-identification

Where Northvale uses aggregated or de-identified information for operational metrics or service improvement, it must apply a de-identification method that makes re-identification not reasonably practicable. The Chief Technology Officer must document the method used. De-identified information that is re-combined with identifiers becomes personal information and is subject to this policy in full.

8. Information Security Safeguards

8.1 Proportionate protection

Safeguards must be proportionate to the sensitivity of the information and the harm that would result from a breach. Patient referral content is Northvale's most sensitive information category and must receive the highest level of protection available within Northvale's control environment.

8.2 Relationship to the Information Security Policy

The technical and organisational controls that protect personal information are set out in the Information Security Policy and the Data Classification and Handling Standard. This policy does not duplicate those requirements. Staff must comply with both instruments.

8.3 Storage and access

Personal information must be stored only in the Northvale platform environment hosted in Azure Canada Central. No copies of personal information may be held on personal devices. Clinician access must be from managed laptops only. Access to personal information must be limited to individuals who need it to perform their role. The Access Control Policy governs how access is granted, reviewed and removed.

8.4 Encryption and transmission

Personal information must be encrypted in transit and at rest. The specific cryptographic requirements are set out in the Data Classification and Handling Standard and the Password and Authentication Standard.

8.5 Physical and environmental controls

Northvale must ensure that personal information is not accessible in physical form in unsecured locations. Printed referral content must be treated as sensitive and disposed of securely.

9. Data Subject Rights

9.1 Northvale's role

Northvale processes patient referral content as a service provider to the referring practice. The referring practice is the custodian of that information under applicable Ontario privacy law. Patients who wish to exercise rights in relation to their referral information — including access, correction or complaint — must direct their request to the referring practice. Northvale does not respond directly to patients on matters where the referring practice is the custodian.

9.2 Northvale's obligation to support

When a referring practice receives a patient request and requires Northvale's assistance to fulfil it, Northvale must provide that assistance within a period set by Northvale and recorded in the written agreement with the referring practice. Northvale has not yet set this internal target;

10 business days from receipt of the practice's request is offered as a starting point and is not derived from any cited control. Northvale must set and record this target before this policy takes effect.

9.3 Clinician rights

Clinicians who hold platform accounts may request access to or correction of their account data by contacting the Chief Technology Officer. Northvale must respond to such requests within a period set by Northvale and recorded in its processing record. Northvale has not yet set this target; 10 business days from receipt is offered as a starting point and is not derived from any cited control. Northvale must set and record this target before this policy takes effect.

9.4 Complaints

Any individual who believes Northvale has not handled their personal information in accordance with this policy or applicable law may raise a complaint. Complaints must be directed to the Chief Technology Officer. The Chief Technology Officer must acknowledge the complaint, investigate it, and provide a written response within a period set by Northvale. Northvale has not yet set this response target; 30 calendar days from receipt is offered as a starting point and is not derived from any cited control. Northvale must set and record this target before this policy takes effect.

If the complainant is not satisfied with Northvale's response, they may escalate to the applicable regulatory authority. Northvale's legal reviewers must confirm which regulatory authority applies to Northvale's operations under applicable Ontario privacy law.

10. Suppliers and Third-Party Processors

10.1 Supplier risk tiers

Northvale classifies suppliers that handle personal information into two tiers:

Critical: any supplier that processes patient referral content or hosts the Northvale platform.

Elevated: any supplier with access to clinician account data.

10.2 Review before onboarding

No Critical supplier may be onboarded without a completed privacy assessment under Section 6 and review by the Chief Executive Officer. No Elevated supplier may be onboarded without a completed privacy assessment reviewed by the Chief Technology Officer. The Third-Party AI

Review Procedure applies where the supplier operates AI systems that interact with personal information. The Third-Party Risk Management Policy governs the broader supplier risk process.

10.3 Mandatory contract terms

Every agreement with a supplier that processes personal information must include:

- (a) a requirement that data is stored and processed within Canada;
- (b) a prohibition on using Northvale's personal information to train, fine-tune or evaluate any AI or machine learning model;
- (c) a requirement that the supplier notifies Northvale of a suspected or confirmed privacy breach within a deadline set by Northvale and recorded in the agreement. Northvale has not yet set this deadline; 24 hours from the supplier's discovery of the event is offered as a starting point and is not derived from any cited control. Northvale must set and record this deadline before executing any supplier agreement;
- (d) a requirement that the supplier names all subprocessors and obtains Northvale's written agreement before adding or changing a subprocessor;
- (e) a requirement that the supplier provides evidence of its controls on a cycle set by Northvale and recorded in the agreement. Northvale has not yet set this cycle; annually is offered as a starting point and is not derived from any cited control;
- (f) a requirement that the supplier certifies the deletion of all Northvale personal information at contract exit, within a deadline set by Northvale and recorded in the agreement.

10.4 Ongoing monitoring

The Chief Technology Officer must maintain a register of all suppliers that process personal information, their tier classification, and the status of their contractual and control obligations. Critical suppliers must be reviewed on a cycle set by Northvale; annually is offered as a starting point and is not derived from any cited control. Elevated suppliers must be reviewed on a cycle set by Northvale; every two years is offered as a starting point and is not derived from any cited control. Northvale must set and record both cycles before this policy takes effect.

11. Cross-Border Transfers and Data Residency

11.1 Canada residency requirement

Personal information processed by Northvale must remain within Canada. This applies to storage, processing, backup and any transfer to a supplier or subprocessor. The current platform environment in Azure Canada Central satisfies this requirement; any change to that environment must be assessed under Section 6 before it is made.

11.2 Transfers outside Canada

No personal information may be transferred outside Canada without prior written agreement from the Chief Executive Officer and a completed privacy assessment confirming that the transfer is lawful under applicable Ontario privacy law. Northvale's legal reviewers must confirm the conditions under which such a transfer would be lawful before any such transfer is contemplated.

11.3 Supplier residency obligations

Every supplier agreement must include the data residency requirement set out in Section 10.3(a). The Chief Technology Officer must verify compliance with this requirement as part of the supplier monitoring process in Section 10.4.

12. Retention and Disposal

12.1 Retention periods

Personal information must not be retained beyond the period necessary for the purpose for which it was collected, or beyond any period required by applicable law or the written agreement with the referring practice. Retention periods for each category of personal information must be set by Northvale, documented in the processing record maintained under Section 5.3, and aligned with the Records Retention and Disposal Policy. Northvale has not yet set these periods; its legal reviewers must confirm the minimum and maximum retention periods applicable to patient referral content and clinician account data under applicable Ontario privacy law before periods are finalised.

12.2 Disposal

When personal information reaches the end of its retention period, it must be disposed of securely and in a manner that makes recovery not reasonably practicable. The method of disposal must be recorded. The Data Classification and Handling Standard sets the technical requirements for secure disposal.

12.3 Supplier deletion at exit

When a supplier agreement ends, the supplier must certify the deletion of all Northvale personal information within the deadline set in the agreement under Section 10.3(f). The Chief Technology Officer must retain that certification.

SPECIMEN

13. Privacy Incidents

13.1 What constitutes a privacy incident

A privacy incident is any event — confirmed or suspected — involving unauthorised access to, collection, use, disclosure, retention or disposal of personal information, or any failure of a control that protects personal information. This includes incidents caused by staff, by suppliers, or by technical failure.

13.2 Reporting

All staff must report a suspected or confirmed privacy incident to the Chief Technology Officer immediately on becoming aware of it. Delay in reporting is itself a policy breach.

13.3 Response

The Privacy Breach Response Procedure governs how Northvale responds to a confirmed or suspected privacy incident. The Security Incident Response Procedure applies where the incident also involves a security event. The AI Incident Response Procedure applies where the incident involves an AI system. All three may apply to the same event.

13.4 Notification

Where a privacy incident may require notification to a referring practice, a data subject, or a regulatory authority, the Chief Technology Officer must assess that obligation promptly and act in accordance with applicable Ontario privacy law. Northvale's legal reviewers must confirm the notification obligations and timelines that apply to Northvale's operations before this policy takes effect.

13.5 Record

The Chief Technology Officer must maintain a record of every privacy incident, the assessment carried out, the actions taken, and the outcome. That record must be retained for a period set by Northvale and aligned with the Records Retention and Disposal Policy.

14. Training and Awareness

All staff who handle personal information must complete privacy training before they are given access to personal information, and on a cycle set by Northvale thereafter. Northvale has not

yet set this cycle; annually is offered as a starting point and is not derived from any cited control. Northvale must set and record this cycle before this policy takes effect.

Training must cover: the categories of personal information Northvale holds; the purposes for which it is processed; staff obligations under this policy; how to recognise and report a privacy incident; and the consequences of non-compliance.

The Chief Technology Officer must maintain a record of training completion. Completion rates must be reported to the Chief Executive Officer as part of the annual review under Section 15.

15. Policy Review and Metrics

15.1 Review cycle

The Chief Technology Officer must review this policy annually and present it to the Chief Executive Officer for review. The Chief Executive Officer's review must be recorded. The review must assess whether the policy remains accurate, complete and effective in light of changes to Northvale's operations, its supplier relationships, applicable law, and the privacy incident record.

15.2 Metrics

The following metrics must be tracked and reported to the Chief Executive Officer at each annual review:

- (a) Privacy requests completed within the target response period set under Section 9.
- (b) Percentage of active processing activities with a documented purpose and lawful basis in the processing record.
- (c) Percentage of required privacy assessments and supplier reviews completed on time.
- (d) Number of exceptions to this policy that have passed their expiry date without renewal or closure.
- (e) Number of material control failures and the number of corrective actions that are overdue.

15.3 Exceptions

Any exception to a requirement in this policy must be requested in writing to the Chief Technology Officer, who must assess the risk and record the outcome. Exceptions that affect

patient referral content require review by the Chief Executive Officer. Every exception must state an expiry date. Exceptions must not be renewed without a fresh assessment.

16. Breaches of This Policy

A breach of this policy is a serious matter. Confirmed breaches will be investigated. Where a breach involves personal information, the Privacy Breach Response Procedure applies. Disciplinary consequences for staff may include termination of employment or engagement. Where a breach involves a supplier, Northvale will exercise its contractual rights, which may include termination of the supplier agreement.

Northvale will not penalise any individual for reporting a suspected privacy incident or policy breach in good faith.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	The organisation has not set the internal response target for supporting a referring practice's patient access or correction request. Section 9.2 offers 10 business days as a starting point. This must be set and recorded before the policy takes effect.	Section 9.2
gap	The organisation has not set the response target for clinician account data requests. Section 9.3 offers 10 business days as a starting point. This must be set and recorded before the policy takes effect.	Section 9.3
gap	The organisation has not set the complaint response target. Section 9.4 offers 30 calendar days as a starting point. This must be set and recorded before the policy takes effect.	Section 9.4
gap	The organisation has not set the supplier breach notification deadline. Section 10.3(c) offers 24 hours as a starting point. This must be set and recorded in every supplier agreement before execution. Note: the customer's stated requirement of '24-hour breach notification' in their answers is a commercial position they intend to impose on suppliers; it is not derived from a cited framework control and is treated here as an organisational parameter to be confirmed.	Section 10.3(c)
gap	The organisation has not set the cycle for supplier control evidence. Section 10.3(e) offers annually as a starting point. This must be set and recorded in supplier agreements.	Section 10.3(e)
gap	The organisation has not set the deadline for certified deletion at supplier exit. Section 10.3(f) requires this to be set and recorded in each agreement.	Section 10.3(f)

gap	The organisation has not set the review cycle for Critical and Elevated suppliers. Section 10.4 offers annually for Critical and every two years for Elevated as starting points. These must be set and recorded before this policy takes effect.	Section 10.4
gap	Retention periods for patient referral content and clinician account data have not been set. Section 12.1 requires legal review to confirm the minimum and maximum periods applicable under Ontario privacy law before periods are finalised. The Records Retention and Disposal Policy must then reflect those periods.	Section 12.1
gap	The retention period for the privacy incident record has not been set. Section 13.5 requires this to be set and aligned with the Records Retention and Disposal Policy.	Section 13.5
gap	The training recurrence cycle has not been set. Section 14 offers annually as a starting point. This must be set and recorded before this policy takes effect.	Section 14
gap	The applicable Ontario privacy legislation and the regulatory authority with supervisory jurisdiction over Northvale's operations have not been confirmed. Candidate instruments for legal review include PHIPA (Personal Health Information Protection Act), PIPEDA or its successor, and any sector-specific regulation applicable to health technology service providers in Ontario. Legal reviewers should confirm which instruments apply and what notification obligations and timelines they impose. This is a candidate list for legal review, not a determination of applicable law.	Sections 9.4, 11.2, 12.1, 13.4
gap	The organisation's locations are listed as 'Not specified'. If Northvale has staff or operations outside Ontario, the cross-border transfer requirements in Section 11 and the applicable law analysis may need to be extended. Legal reviewers should confirm.	Section 11
vague	The customer's answers describe the privacy-request process as directing patients to the referring practice and supporting the practice within 10 business days. It is not clear whether this 10-business-day figure is a current operational commitment or an aspirational target. Section 9.2 treats it as a starting point for an organisational parameter to be formally set. The organisation should confirm the intended figure.	Section 9.2
gap	The sibling document 'Records Retention and Disposal Policy' is referenced in Sections 12 and 13.5. This policy cannot assert what retention periods that instrument sets. The organisation must reconcile the retention periods set under Section 12.1 of this policy with whatever that instrument already states.	Sections 12.1, 13.5
gap	No verified framework was supplied. This policy is written to RiskWoven AI practical best practices. No framework control identifiers have been cited. The organisation should confirm that this basis is sufficient for its regulatory and contractual obligations.	Throughout

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- The internal target for Northvale to support a referring practice's patient access or correction request (Section 9.2). 10 business days is offered as a starting point.
- The response target for clinician account data requests (Section 9.3). 10 business days is offered as a starting point.
- The complaint response target (Section 9.4). 30 calendar days is offered as a starting point.
- The supplier breach notification deadline to be written into every supplier agreement (Section 10.3(c)). 24 hours is offered as a starting point.
- The cycle for suppliers to provide evidence of controls, to be written into supplier agreements (Section 10.3(e)). Annually is offered as a starting point.
- The deadline for certified deletion of Northvale personal information at supplier exit, to be written into each agreement (Section 10.3(f)).
- The review cycle for Critical suppliers (Section 10.4). Annually is offered as a starting point.
- The review cycle for Elevated suppliers (Section 10.4). Every two years is offered as a starting point.
- Retention periods for patient referral content and clinician account data, confirmed by legal review against applicable Ontario privacy law and aligned with the Records Retention and Disposal Policy (Section 12.1).
- The retention period for the privacy incident record, aligned with the Records Retention and Disposal Policy (Section 13.5).
- The training recurrence cycle for staff who handle personal information (Section 14). Annually is offered as a starting point.
- Legal confirmation of which Ontario privacy legislation applies to Northvale's operations (candidates include PHIPA and PIPEDA or its successor), the regulatory authority with supervisory jurisdiction, and the notification obligations and timelines that apply to privacy incidents (Sections 9.4, 11.2, 12.1, 13.4).
- Confirmation of all locations where Northvale has staff or operations, to determine whether the cross-border transfer requirements in Section 11 need to be extended (Section 11).
- Reconciliation of the retention periods set under this policy with any periods already stated in the Records Retention and Disposal Policy (Sections 12.1, 13.5).
- Confirmation that the 'Chief Technology Officer' and 'Chief Executive Officer' role titles used throughout this policy match Northvale's current organisational structure and that

named individuals in those roles have accepted the accountabilities assigned.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

SPECIMEN