Lumeval — Security & Data Handling Overview

How pilot data is requested, transferred, protected, and destroyed · lumeval.com

Data minimization by design

The pilot begins with a de-identified case-list export only. No worker names, dates of birth, addresses, social insurance numbers, health card numbers, or other direct identifiers are requested at intake. Clinical documents are requested only for the 30 selected cases, only to the extent needed for review, and are handled under the principles below.

Privacy framework

Lumeval operates under Canadian privacy law, including PIPEDA and applicable provincial legislation (e.g., BC PIPA, Alberta PIPA/HIA). Engagements are governed by a written agreement covering purpose limitation, confidentiality, permitted use, and data return or destruction. Where the client requires it, Lumeval will execute the client's information-sharing or data-processing agreement. Individual clinical information remains clinically governed; employer-facing reporting is aggregate and de-identified with small-cell suppression.

Transfer, storage, and access

- Secure transfer arranged directly with each client (client-provided SFTP or a secure portal agreed at kickoff). No case documents accepted by email.
- Data stored encrypted at rest and in transit on Canadian-resident infrastructure.
- Access restricted to the reviewing physician and named engagement staff under confidentiality agreements; access is logged.
- Client data is segregated per engagement; no commingling across clients.

How AI is used — and not used

AI assists with document organization: timeline extraction, classification of stuck-case categories, and drafting of accountability-map fields. Every map is reviewed and finalized by a physician before delivery. AI does not make autonomous claim, entitlement, fitness-for-duty, or medical-legal determinations. AI tooling is configured so client data is not used to train third-party models.

Retention and destruction

Case documents are retained only for the duration of the engagement plus a short contractual wind-down period (typically 60 days), then destroyed with written confirmation. De-identified, aggregate findings (e.g., bottleneck category counts) may be retained for benchmarking only where the engagement agreement permits.

Incident response

Suspected privacy or security incidents are contained, assessed, and reported to the client without unreasonable delay, with breach notification handled in accordance with PIPEDA and applicable provincial requirements.

Worker-trust commitments

- No individual worker dashboards and no employer access to individual worker medical information.
- No claims adjudication, no IMEs, no fitness-for-duty assessments, no credibility or fraud scoring.
- Outputs are designed to reduce case drift — no worker left in limbo because the next step is unclear.

Questions or security review requests: dan@lumeval.com. This overview is informational and does not replace the engagement agreement. Specific transfer methods, retention periods, and tooling are confirmed in each engagement agreement.