

PRIVACY AND SECURITY INCIDENT RESPONSE PROTOCOL

Every clinic agreement commits DentaVate to notify at the first reasonable opportunity. That promise needs a process behind it or it is a liability rather than a control.

1. What counts as an incident

Information sent to the wrong person • the wrong patient contacted • access to a record the person was not authorized to see • a lost or stolen device • suspected phishing or malware • an unexpected or unrecognized login • a screenshot or photograph of patient information • credential compromise • patient information entered into an unapproved tool • any suspected unauthorized access, use, disclosure, or loss.

Suspected counts. Nobody has to be certain before reporting.

2. Immediate steps

Step	Who
Stop work; do not attempt to fix or delete anything	Person who noticed
Report to the Privacy Officer immediately	Person who noticed
Preserve evidence — logs, screenshots of the error, the affected record reference	Privacy Officer
Suspend or revoke access where compromise is possible	Privacy Officer
Rotate credentials where relevant	Privacy Officer
Open a register entry	Privacy Officer

Reporting promptly and in good faith is never a basis for adverse consequences. **Concealing an incident, or quietly correcting one, is a serious breach.**

3. Notifying the clinic

At the **first reasonable opportunity**. A preliminary notice may be given while investigation continues, with further information as it becomes available.

The notice states: what is known, what is not yet known, what has been contained, what DentaVate is doing next, and what the clinic may need to consider.

It also states that **notice is not an admission that a privacy breach occurred under any statute, and does not determine responsibility.**

4. Who notifies whom

The **clinic** decides whether to notify patients, a privacy commissioner, or its college, and makes that notification. It is the trustee, custodian, or organization under its provincial law.

DentaVate provides the information reasonably necessary to support that decision, and makes its own report where PIPEDA obligations apply to information under DentaVate's control.



Provincial triggers differ. Do not apply one province's rule to another clinic.

5. The register

Every breach of security safeguards is recorded, **whether or not it is reportable**, and kept for at least 24 months. This is a PIPEDA obligation independent of anything in a clinic agreement.

Each entry: date, date discovered, description, information involved, number of individuals affected, cause, containment steps, whether a real risk of significant harm was assessed, whether notification was made and to whom, and the person who recorded it.

The register holds **the minimum patient detail necessary to describe the incident**. It is not a copy of the affected records.

6. After

A short review: what happened, why, what changes. Where a control failed, the fix goes into the Workspace Policy or the Worktable rules as a new version.

7. Roles

Role	Person
Privacy Officer	{{privacy_officer_name}}
Backup	{{privacy_officer_backup}}
Breach counsel	{{breach_counsel}}
Cyber insurer notification	Per policy ZMC25362 — notify promptly; late notice can prejudice coverage

