



PERSONAL DATA BREACH RESPONSE PLAN

What to do in the first hours and days after personal data is lost, exposed or misused

Document No.: CYD-DP-05 | Version 1.0 | Effective date: November 5, 2026 | Owner: Zebroid Private Limited | Status: Approved

1. Purpose

A personal data breach is any event that leads to the accidental or unlawful loss, alteration, disclosure of or access to personal data. This plan makes sure that every breach is contained quickly, assessed honestly and notified on time. Health data makes the harm of a breach especially serious.

2. Response team

Role	Name and contact
Incident lead (director)	
Data protection lead / DPO	
Technical lead	
Medical lead	
Legal adviser	
Communications	

3. Steps

- Detect and report.** Anyone who suspects a breach reports it at once to the technical lead and the data protection lead. Nobody waits to be sure.
- Contain.** Stop the cause: disable accounts, revoke keys, isolate systems, recall messages. Preserve evidence.
- Assess.** Find out what data, whose, how many people, how it was exposed and whether it is still at risk. Rate the risk to individuals as low, medium or high.
- Notify.** Follow the table below.
- Recover and support.** Restore systems, help affected people, and, where harm to health is possible, ask the medical lead to contact them.
- Review.** Within 30 days, write a report on the cause and the corrective steps, and update policies and training.

4. Notification

Who	When	Source of duty
Supervisory authority in the EU (for data of people covered by the GDPR)	Without undue delay, and where feasible within 72 hours of becoming aware, unless the breach is unlikely to risk individuals' rights	General Data Protection Regulation
Individuals in the EU	Without undue delay where the risk is high	General Data Protection Regulation
Data Protection Board of India and each affected person (for data covered by India's law)	As the Digital Personal Data Protection Rules require, including a prompt first notice and a fuller report within the prescribed time	Digital Personal Data Protection Act and Rules
Controllers, hospitals or centres for whom we process data	As the contract requires, and at once	Contract



Who	When	Source of duty
Police or other authorities	Where the breach involves a crime	Legal adviser's decision

The legal adviser confirms the exact time limits at the time of each breach.

5. Breach log

Every breach, including those that are not notified, is entered in the breach log with its date, description, data and people affected, risk rating, decisions on notification and reasons, and corrective steps. The log is kept for six years.

6. Examples of breaches

- A prescription or report sent to the wrong person by message or email.
- A lost or stolen laptop or phone containing patient information, or an unlocked screen seen by others.
- An attacker or malware gaining access to the platform, or ransomware encrypting records.
- A vendor or partner losing or exposing data that it holds for the company.
- An employee or doctor looking at a record without a reason, or copying records.
- A system fault that makes one patient's records visible to another.

7. Risk rating

Rating	Meaning	Typical response
Low	Little chance of harm, for example data encrypted and the key safe, or an error corrected before use	Log, correct, no notification unless required
Medium	Some chance of harm to a limited number of people	Notify the authority where required; consider telling individuals
High	Likely harm, for example health data exposed, or large numbers of people affected	Notify the authority and tell individuals without delay; offer support

8. Information for notices

- What happened, when it was found and whether it is over.
- The kinds of data and the number of people and records involved.
- The likely consequences for the people affected.
- What the company has done and will do, and how people can protect themselves.
- A contact point for questions, such as the grievance officer or the data protection lead.

9. Training and testing

All staff and doctors are told how to recognise and report a breach when they join and each year. Once a year the response team carries out a practice exercise based on a realistic scenario, such as ransomware or a message sent to the wrong patient, and records what it learned and what was changed.

10. Contacts and authorities

Authority	Contact details
Supervisory authority in the EU member state concerned	



Authority	Contact details
Data Protection Board of India	
Cyber incident authority, where applicable	
Insurer	
Police	

11. Deciding whether to notify

1. Confirm that personal data was affected.
2. Identify which laws apply, according to where the people live and where the data is held.
3. Rate the risk to people and compare it with the legal test for notification in each law.
4. Record the decision, the reasons and who took it. If in doubt, take advice and lean towards notifying.
5. If the decision is not to notify, record why, and keep the record.

12. Review checklist

- Was the breach found quickly? If not, why?
- Did people know whom to call?
- Were containment and notification on time?
- Were patients and doctors given clear information?
- What must change in systems, vendors, training or policies?
- Have actions been entered in the plan with owners and dates?

13. Support for affected people

Where a breach may harm people, the company offers clear advice on what they can do, such as changing passwords, watching for suspicious messages or contacting their bank. Where health information is exposed, the medical lead makes sure that anyone who might be harmed by the exposure, or who is worried, can speak to a doctor. The company answers questions promptly and kindly.

14. Records

All records of a breach, including the log, the evidence, the assessment, the decision on notification, copies of notices and the review report, are kept for six years in a secure place, and are made available to a regulator on request.

Approval

This document is approved by the directors of Zebrold Private Limited, the operator of Consult Your Doctor.

Hemendrah Kumar Sadamsetty

Electronically signed | November 5, 2026

Hemendrah Kumar Sadamsetty

Director, Zebrold Private Limited

Date: November 5, 2026

Indu Reddy Morthala

Electronically signed | November 5, 2026

Indu Reddy Morthala

Director, Zebrold Private Limited

Date: November 5, 2026