



INFORMATION SECURITY AND ACCESS CONTROL POLICY

How patient and company information is protected, and who can see what

Document No.: CYD-SEC-01 | Version 1.0 | Effective date: November 5, 2026 | Owner: Zebrold Private Limited | Status: Approved

1. Purpose and scope

This policy protects the confidentiality, integrity and availability of the information of Zebrold Private Limited and of the patients of Consult Your Doctor. It applies to all staff, doctors, diagnostic centres, contractors and vendors who use the platform or its systems.

2. Responsibilities

The directors are accountable for security. The technical lead runs the security programme, and the data protection lead advises on privacy. Everyone must follow this policy and report anything suspicious at once.

3. Access control

Access is given on the basis of need and role, approved by the owner of the information, and removed on the day a person leaves or changes role. Access rights are reviewed every quarter.

Role	Access
Patient	Own records only
Doctor	Records of own patients and those they are covering; no export of records
Diagnostic centre user	Test requests and reports for patients referred to the centre
Support staff	Contact and booking details; no clinical content unless needed and approved
Medical lead and quality staff	Clinical records needed for audit, with every access logged
Administrators and developers	Systems and test data only; production patient data only by approved, time-limited access

4. Technical controls

- Multi-factor authentication for all staff and doctors, and for any administrative access.
- Encryption of data in transit and at rest, with keys managed separately and rotated.
- Unique accounts; no shared logins; strong passwords stored in an approved manager.
- Logging of access to patient records, kept for at least one year and reviewed for unusual activity.
- Regular security updates, vulnerability scanning each month and an independent penetration test every year.
- Daily backups, stored separately and tested for restore every quarter.
- Separate development, testing and production environments; real patient data is not used for testing.

5. People

Everyone with access signs a confidentiality undertaking and receives security and privacy training when they join and every year. Doctors and diagnostic centres agree to the same standards in their contracts.



6. Vendors

No vendor receives access to personal data until its security has been reviewed and a data processing agreement has been signed. Vendors are reviewed every year.

7. Incidents

Security incidents are reported to the technical lead immediately and handled under the Personal Data Breach Response Plan (CYD-DP-05).

8. Incident classification

Level	Examples	Response
Critical	Patient data exposed; ransomware; platform down	Immediate response; directors informed; breach plan (CYD-DP-05)
High	Suspected misuse of an account; serious vulnerability found	Respond within 4 hours
Medium	Phishing reports; a lost device with encryption	Respond within 1 working day
Low	Policy breaches without exposure of data	Respond within 5 working days

9. Physical security

Offices have controlled entry, visitor logs and locked storage for paper records. Screens are positioned and locked so that patient information is not visible to visitors. Paper records are kept to a minimum and shredded when no longer needed. Servers and network equipment are in secure areas, or are in the data centres of vendors that meet recognised security standards.

10. Change management and development

- Every change to the platform is requested, reviewed, tested in a separate environment and approved before release, and can be reversed.
- Code is reviewed by a second developer, and automatic checks look for known vulnerabilities and exposed secrets.
- Security requirements are part of the design of every new function, and a privacy review is done where personal data is involved.
- Emergency changes are recorded and reviewed afterwards.

11. Mobile and remote working

Mobile devices that access company data are enrolled in device management, protected by a passcode and encryption, and can be wiped remotely. Staff working remotely use only secure networks and the company's virtual private network and must follow the IT and Acceptable Use Policy (CYD-SEC-02).

12. Disposal of equipment and data

Devices and storage that are no longer needed are wiped to a recognised standard or physically destroyed, and a certificate or record is kept. Cloud resources are deleted through documented steps, and keys are destroyed where the data is to be made unreadable.



13. Security awareness and training

All people with access to company systems take security training when they join and then every year. The training covers phishing and social engineering, password and device safety, the handling of patient data, reporting incidents and the consequences of breaches. Technical staff receive extra training on secure development and incident response. The company runs simulated phishing tests and uses the results to improve training.

14. Monitoring and audit

The technical lead monitors systems for unusual activity and reviews access logs. An independent audit or penetration test is carried out every year, and the results and the actions taken are reported to the directors. Internal checks on access rights, backups and patching are made every quarter.

15. Third-party access

Access by vendors, auditors and partners is allowed only to the extent and for the time needed, through named accounts with multi-factor authentication, and is logged. Remote support sessions are supervised by a member of staff.

16. Exceptions

An exception to this policy may be granted only in writing by the technical lead and the data protection lead, for a stated period, with the risk assessed and measures put in place. All exceptions are recorded and reviewed every quarter.

17. Encryption and key management

Data is encrypted in transit using current, strong protocols and at rest using strong algorithms. Keys are generated, stored and rotated in a managed key service that is separate from the data, and access to keys is limited to a small number of named administrators. Keys are changed after a suspected compromise and when administrators leave.

18. Logging

Systems record who accessed or changed patient records, from where and when, and the logs are protected from alteration. The technical lead reviews alerts for unusual patterns, such as access outside working hours, mass downloads or access to the records of colleagues, and investigates every alert.

19. Review

The technical lead reviews this policy every year and after any serious incident.

Approval

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

Hemendrah Kumar Sadamsetty

Electronically signed | November 5, 2026

Hemendrah Kumar Sadamsetty

Director, Zebroid Private Limited

Date: November 5, 2026

Indu Reddy Morthala

Electronically signed | November 5, 2026

Indu Reddy Morthala

Director, Zebroid Private Limited

Date: November 5, 2026