At Laptis, protecting patient data is not just a requirement – it is one of our core values. Accordingly, we've outlined our security practices below.

Governance, Risk & Compliance

- **HIPAA Compliance**: Laptis is fully compliant with HIPAA. We meet and maintain all HIPAA requirements through secure systems, policies, and practices.
- **42 CFR Part 2 Compliance**: Laptis is fully compliant with 42 CFR Part 2. We meet and maintain all 42 CFR Part 2 requirements through secure systems, policies, and practices.
- **SOC 2 Reports**: We regularly conduct SOC 2 Type 2 audits which evaluate our sufficiency across all five trust services criteria. Our most recent audit letter came in December 2025 and found us in full satisfaction of all five trust services criteria.
- **Vendor BAAs**: Every vendor that handles PHI has a signed Business Associate Agreement (BAA), ensuring they are legally accountable to the same standards we uphold.
- **Regulatory Tracking**: We continuously monitor compliance obligations and review internal policies, ensuring every change follows a standardized, secure process.
- **Risk Management**: A centralized risk register guides how we identify, assess, mitigate, and monitor risks across the organization.

Workforce Security

- **Company-wide Training**: Every employee is trained in security best practices, with annual refreshers and additional training after any major operational change.
- **Personal System Security**: Employees use secure tools including VPNs, password managers, malware protection, and device-level encryption to ensure devices that access PHI and PII are robustly protected.

Data Protection & Infrastructure

- **Data Protection**: All data is encrypted both while moving and while stored, traveling only through secure channels. Access is strictly limited to authorized individuals on a "need to know" basis.
- **Network Security**: Only the application layer communicates with the database, which drastically minimizes the risk of compromise. We keep that connection safe by using private networks and only allowing approved devices to connect.
- **High Availability**: Our systems are designed for resilience and continuous performance, with proactive monitoring to minimize downtime.
- **Backup & Disaster Recovery**: We maintain secure backups and have a tested disaster recovery plan to restore access quickly if systems are disrupted.
- **Authorization & Privilege**: Role-based access controls ensure the right people have the right level of access, and nothing more. These controls are reviewed quarterly.

System Testing & Monitoring

- **Secure Software Development**: All updates are reviewed, tested, and scanned for vulnerabilities before release. Issues are tracked and resolved within defined timelines.

- **Penetration Testing**: Independent third-party security experts conduct annual "ethical hacking" tests to identify vulnerabilities which we subsequently patch up. Our most recent test was completed in April 2026.
- **Monitoring & Detection**: We track and record everything happening in our systems so we always have full visibility into performance and security.

Vendor Oversight

- **Vendor Assessments**: All vendors are thoroughly vetted before engagement, including a review of data access, security controls, certifications, and breach history.
- **Access Control**: Vendors receive the bare minimum access required for their role.
- **Ongoing Monitoring**: Vendors are reassessed annually, with continuous contract monitoring and access reviews. Upon termination, access is revoked immediately and data is securely deleted or returned per contract.
- **Vendor Accountability**: We hold all vendors to the same standards we hold ourselves.