SECURITY & PATIENT PRISM
PROTECTING YOUR DATA

Patient Prism

Our Priority is Your Protection

While modern technologies unleash tremendous advancements, we live in a world with unending security risks. Patient Prism focuses relentlessly on security in its people, processes, and technology.

We implement layers of security controls to ensure that your data remains confidential, that your data remains correct and unaltered, and that systems are up and running continuously.

PatientPrism uses leading edge technology for marketing and practice automation – and our security technologies are equally advanced – all designed to protect your business.

Layers of Protection

Patient Prism's layers of protection include security leadership and governance, identity and access management, incident detection and response, cryptographic protection, human resource security, and much more.

Security Leadership and Governance

Human Resource Security

IT Asset Management

Access Controls

Cryptography

Physical Security

Operational Security

Network Security

Third-Party Management

Security Detection and Response

Business Continuity and Disaster Recovery

Innovation in Security

Bad actors are constantly evolving. Threats change quickly. Patient Prism's security program keeps pace with the threat landscape, constantly evolving with new safeguards to protect your data. Our security approach includes:

THREAT INTELLIGENCE » ONGOING TRAINING » BEST-IN-CLASS TECHNOLOGY

24/7 Peace of Mind

Patient Prism has invested in comprehensive, 24x7 threat monitoring, including both highly-trained security specialists plus AI-powered analysis of data, to ensure that your data is protected.

PROTECTIONS INCLUDE:

Continuous Server & Workstation Scanning

Daily vulnerability scans of firewalls

Security Awareness Training for staff with simulated phishing

Regular Penetration Testing

AI-powered advanced threat detection and

Continual monitoring via advanced visibility platform combined with timely remediation

A business partner that you can count on

» Continuous investments in security technology to stay ahead of security threats

» Program built on most up-to-date security frameworks

» Collaboration with law enforcement and data protection authorities in the North America, UK, and Europe

Technical and Operational Security Measures

See below for Patient Prism's comprehensive set of technical and operational security measures:

Information Security Management Process

- Top Management Leadership of Security Team
- Regular Risk Assessments
- Information Security Policy
- Remediation of Risks

Human Resource Security

- Screening/Background Checks
- Employee Security Agreements
- Staff Security Training
- Robust Termination Procedures

Data Governance and IT Asset Management

- Data Classification
- Asset Inventory
- Data Destruction

Access Controls

- Access using Principle of Least Privilege
- Tight Controls for Privileged Access Rights
- Secrets Management using State of Art Tools
- Periodic Audit of Access Rights
- Access Removal

Cryptography. AES 256 used for Data at Rest

Physical and Environmental Security

- Physical Security Program
- Work from Home Policies
- Data Center Security – Rigorous Security by Major Cloud Providers

Operational Security

- Threat Intelligence
- Change Management
- Device Management
- Protection from Malware
- Patching
- Data Backup and Recovery
- Logging and Monitoring
- Vulnerability Management

Network Security

- Secure System Design
- Secure Configuration
- Security Testing

Data Transmission Control and Encryption - Use TLS 1.2 or better

System Development and Maintenance

- Secure System Development
- Separation of Environments
- Secure Development Environment
- System Security Testing

Third Party Management

- Contracting Guidelines
- Vendor Security Policy
- Third-Party Risk Management

Security Incidents and Response Plan

Business Continuity and Disaster Recovery

AT PATIENT PRISM
YOUR DATA IS SECURE

Patient Prism