Healthcare & Regulated Sectors Guide

Patient Confidentiality & Data Protection

Healthcare organizations process highly sensitive patient information requiring stringent security controls and regulatory compliance. Stannp operates as a Data Processor under PIPEDA and Canadian privacy laws, providing the security framework necessary for protecting patient and healthcare communications data.

All patient and healthcare communications data receives confidential classification with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. Data hosting occurs exclusively within Canada (Canada Central and Canada East regions) on Microsoft Azure infrastructure. Authorized UK-based personnel may access data remotely for print file creation and support operations, with all data remaining on Canadian servers. All access is secured through encrypted connections, multi-factor authentication, and comprehensive logging, with personnel contractually bound to maintain PIPEDA-equivalent standards. This ensures complete data residency compliance essential for Canadian healthcare providers and provincial health authorities.

Security Architecture & Access Control

Healthcare organizations manage their own user accounts and access controls within the platform, enabling role-based access control with least privilege and need-to-know principles appropriate to clinical workflows. Multi-factor authentication is available to enhance security for accounts accessing patient data, supporting compliance with provincial health information privacy requirements.

The platform operates continuous monitoring with 99%+ uptime SLA, ensuring healthcare communications including appointment reminders, test results, and care coordination remain accessible. Critical database services maintain RTO 30 minutes and RPO 6 hours, supporting continuity of care communications.

Healthcare Regulatory Compliance

Maintaining ISO 27001 and PCI-DSS certifications demonstrate regulatory compliance appropriate for healthcare sector requirements. Our security program supports provincial health information privacy legislation compliance, and healthcare regulatory expectations for data protection.

Monthly vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses across systems processing patient information. Security assessments are conducted to validate the effectiveness of controls protecting healthcare data.

OWASP Top 10 application security testing protects against common web application vulnerabilities that could compromise patient confidentiality. Automated GitHub vulnerability scanning monitors source

Stannp Inc.
2727 Steeles Avenue West, Suite 1032,
North York, Ontario, M3J3G9, Canada
www.stannp.com
+1 437 295 0300

code continuously. Critical patches are applied within 7 days, important patches within 14 days, and moderate patches within 30 days.

Patient Data Protection & Backup

Critical patient data receives backup every 15 minutes with daily full backups retained for 30 days. All backup data is encrypted and stored in zonally separated locations within Canada, ensuring recovery capability while maintaining strict data sovereignty requirements for patient information.

Organizations manage their own data retention policies within the platform. The system supports 2-month processing retention for PIPEDA and Canadian privacy law erasure rights. Secure disposal procedures include physical destruction of hard drives before disposal, complying with WEEE legislation and ensuring patient data cannot be recovered from disposed equipment.

Incident Response & Breach Management

Data breaches posing a real risk of significant harm are reported to the Office of the Privacy Commissioner of Canada as soon as feasible as required by PIPEDA and Canadian privacy laws. Incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response processes: detection, classification, containment, investigation, eradication, recovery, and post-incident review. Comprehensive incident logs enable pattern identification and continuous improvement.

Staff Training

Staff receive annual security awareness training covering PIPEDA and Canadian privacy laws, phishing, social engineering, and incident reporting.

Stannp Inc.
2727 Steeles Avenue West, Suite 1032,
North York, Ontario, M3J3G9, Canada
www.stannp.com
+1 437 295 0300