Healthcare & Regulated Sectors Guide

Data Protection & Confidentiality

Stannp operates as a Data Processor under UK GDPR and Data Protection Act 2018 with ICO registration ZA134992. All patient and healthcare communications data is classified as confidential and protected with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. Data is hosted exclusively in Ireland (EEA) on Microsoft Azure with no transfers outside the EEA, ensuring complete data residency compliance.

Security Architecture & Access Control

Multi-factor authentication is mandatory for all internal systems with 2-hour session timeouts and unique user credentials. Access follows role-based access control with least privilege and need-to-know principles. The platform operates 24/7 SIEM monitoring with 12-month audit log retention and clock synchronisation. Critical services maintain 99%+ uptime SLA with RTO 30 minutes and RPO 6 hours for databases.

Compliance & Security Testing

ISO 27001, Cyber Essentials, and PCI-DSS certifications demonstrate regulatory compliance. Security programme includes:

- Monthly vulnerability scans using Qualys and Security Scorecard
- Annual penetration testing and security assessments
- OWASP Top 10 application security testing
- Automated GitHub vulnerability scanning for source code
- Critical patches within 7 days, important within 14 days, moderate within 30 days

Data Management & Recovery

Critical data backups occur every 15 minutes with daily full backups retained for 30 days. All backups are encrypted and geographically separated within the EEA. Standard retention is 3 years (customisable) with 2-month processing retention, supporting GDPR erasure rights and secure disposal procedures.

Incident Response & Breach Management

Data breaches are reported to the ICO within 72 hours as required by UK GDPR. 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.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

Physical Security & Staff Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access and visitor accompaniment. Clean desk policy and locked cabinets protect confidential materials. All equipment is tracked throughout its lifecycle with hard drives physically removed and destroyed before disposal, complying with WEEE legislation. Staff receive annual security awareness training covering UK GDPR, phishing, social engineering, and incident reporting. HIPAA training is provided upon induction for relevant personnel with annual updates.