GoodX HEALTHCARE

Secure Practice Blueprint

A Practical Cybersecurity Checklist for Healthcare Providers

bsi
ISO 9001 Quality Management Systems CERTIFIED
ISO/IEC 27001 Information Security Management CERTIFIED
MONITOR
IMPLEMENT
PLAN

Organizational Security

- □ Your EMR vendor holds ISO/IEC 27001:2022 (or equivalent) certification
- □ Regular security risk assessments are conducted
- □ Data protection policies are documented and reviewed annually
- □ All staff receive cybersecurity awareness training
- □ Data retention and secure disposal policies are defined and enforced for PHI (personal health information) and backups
- □ Internal audits are conducted annually to verify compliance with security policies and standards

Technological Controls

- □ Automatic software updates are enabled
- □ Cloud storage follows verified security protocols
- □ Data encryption is applied in transit and at rest
- □ Audit logs are reviewed for suspicious activity
- □ An incident response plan defines roles, reporting procedures, and timelines for breach notifications (aligned with PHIPA requirements)
- □ A disaster recovery plan is in place and tested annually

People & Access

- □ Strong multi-factor authentication (MFA) is in place
- □ User access follows a least privilege model
- □ Employee offboarding includes immediate access revocation
- □ Shared credentials are prohibited

Physical Security

- □ Clinic computers and servers are physically secured
- □ Portable devices are encrypted and locked when unattended
- □ Backup systems are tested regularly

Continuous Improvement

- □ Partner only with certified EMR vendors
- □ Review security policies with vendors yearly
- □ All third-party vendors handling PHI are vetted for compliance with ISO 27001 or equivalent standards
- □ Vendor contracts include confidentiality and breach notification clauses
- □ Stay informed through cybersecurity advisories and updates from Canadian Centre for Cyber Security

This checklist is for guidance; consult experts for full compliance.