Saskatchewan Clinic Cybersecurity Checklist

A one-page, HIPA-aligned IT controls checklist for medical clinics and pharmacies. Hand this to your office manager or use it to interview a prospective IT provider. Updated 2026.

1. Identity & access

- Every staff member has a unique account — no shared logins on any device or system.
- MFA is enforced on Microsoft 365, the EMR, remote access, and the cyber-insurance portal.
- Role-based permissions in the EMR (front desk, clinical, billing, admin) — reviewed annually.
- Account offboarding checklist runs the same day a staff member leaves.

2. Devices & endpoints

- BitLocker (Windows) or FileVault (macOS) enabled on every workstation and laptop.
- Endpoint Detection and Response (EDR) deployed — not just legacy antivirus.
- Operating system and browser auto-updates enabled and verified monthly.
- Workstations refreshed on a 3–4 year cycle; out-of-support OS removed from the network.
- Mobile devices accessing PHI are enrolled in MDM (Intune) with passcode + remote wipe.

3. Network & perimeter

- Business-grade firewall with current firmware and an active support license.
- Separate Wi-Fi network for patient/guest traffic, isolated from the clinical network.
- Remote access via Microsoft Entra ID + Conditional Access or a managed VPN — no exposed RDP.
- DNS filtering blocking known malicious and phishing domains.

4. Microsoft 365 & cloud

- Microsoft 365 Business Premium (or higher) with Canadian-region tenant.
- Email rules: anti-phishing, safe links, safe attachments, external-sender banner.
- Conditional Access blocks sign-ins from outside Canada unless explicitly permitted.
- Audit logging enabled and reviewed quarterly.

5. Backups & recovery

- Image-based backup of EMR server and key workstations, daily.
- At least one immutable / offsite backup copy stored in Canada.
- Restore test performed and signed off at least once per quarter.
- Documented downtime procedure on paper at every workstation.

6. HIPA / PIPEDA governance

- Privacy Officer named in writing; contact details posted at reception.
- Clinic-specific privacy and security policies, signed and reviewed annually.
- Privacy training delivered at hire and annually; signed acknowledgements on file.
- Signed Information Management Service Provider agreement with IT, EMR, backup, and AI scribe vendors.
- Breach response procedure with OIPC notification path documented.
- Certificates of destruction kept for every retired drive, workstation, and paper record.

7. EMR & integrations

- EMR client and database on the supported version; updates applied on a documented cadence.
- Antivirus exclusions configured correctly for the EMR database files; EDR active elsewhere.
- Lab / eFax / PIP / Netcare integrations monitored — outages detected proactively, not by staff.
- AI scribe (if used) has a signed agreement, Canadian data residency, and a documented risk assessment.

Need help running this against your clinic? Book a free 30-minute review at logicdots.ca/assessment and we'll send back a written report scoring you on every item above.