# 2026 Protect Your Practice Checklist

This checklist is designed to help clinicians assess whether basic privacy governance and cybersecurity safeguards are in place. Initiating a tabletop exercise to identify critical needs and gaps for the clinic is a starting point.

| Governance & Accountability | Yes | No |
|---|---|---|
| 1. Have you designated a person responsible for privacy and cybersecurity oversight within the clinic? | ☐ | ☐ |
| 2. Does the clinic maintain current privacy, security policies and procedures and a privacy notice? | ☐ | ☐ |
| 3. Has the clinic performed a privacy and cybersecurity risk assessment in the last 12 months (including for AI tools that may be in use)? | ☐ | ☐ |
| 4. Does the clinic have a documented incident response plan for privacy breaches, ransomware and cyber incidents? | ☐ | ☐ |
| 5. Have you considered obtaining or reviewing cyber liability insurance coverage? | ☐ | ☐ |
| **People & Training** | **Yes** | **No** |
| 6. Do all physicians and staff complete privacy and security training when they join and at least annually thereafter? | ☐ | ☐ |
| 7. Is staff completion of privacy and security tracked and documented? | ☐ | ☐ |
| 8. Are confidentiality obligations built into staff and contractor agreements and communicated? | ☐ | ☐ |
| 9. Is there a process to promptly remove access when a staff member leaves or changes roles? | ☐ | ☐ |
| 10. Are audit logs monitored to identify inappropriate access or "snooping"? | ☐ | ☐ |
| **Technology & Cybersecurity** | **Yes** | **No** |
| 11. Is multi-factor authentication enabled wherever available? | ☐ | ☐ |
| 12. Are strong password requirements enforced and shared accounts prohibited? | ☐ | ☐ |
| 13. Are clinic computers, devices and software regularly updated and patched? | ☐ | ☐ |
| 14. Does the clinic use secure email solutions and avoid transmitting PHI through unsecured email services? | ☐ | ☐ |
| 15. Are staff prohibited from using public Wi-Fi or other unsecured networks to access patient information? | ☐ | ☐ |
| 16. Is patient information encrypted both in transit and at rest? | ☐ | ☐ |
| 17. Is there a printed emergency contact list with EMR vendor, critical staff and support contact information in case of an outage or incident? | ☐ | ☐ |
| **Backups & Business Continuity** | **Yes** | **No** |
| 18. Are critical systems and patient records backed up automatically on a regular basis? | ☐ | ☐ |
| 19. Are backups tested annually to confirm that data and systems can be restored successfully? | ☐ | ☐ |
| 20. Does the clinic have a plan to continue operations during a cyber incident or system outage? | ☐ | ☐ |
| **Vendors & AI Governance** | **Yes** | **No** |
| 21. Have you completed due diligence on all vendors that handle patient information? | ☐ | ☐ |
| 22. Do vendor contracts address privacy, security, breach notification, audit rights, retention and destruction of PHI? | ☐ | ☐ |
| 23. Before adopting an AI tool, have you confirmed where PHI is stored, whether it is retained, and whether it is used to train models? | ☐ | ☐ |
| 24. Before adopting an AI tool, have you assessed vendor safeguards, contractual protections and incident management processes? | ☐ | ☐ |
| 25. Do clinicians review AI-generated outputs and remain accountable for clinical decisions? | ☐ | ☐ |
| 26. Where available, have you considered using solutions that have undergone sector-specific procurement and privacy/security review processes (e.g. VOR programs)? | ☐ | ☐ |

*Stay up to date on your privacy and security obligations by taking OntarioMD's complimentary, accredited training at [https://www.ontariomd.ca/products-and-services/privacy-and-training-resources/overview](https://www.ontariomd.ca/products-and-services/privacy-and-training-resources/overview).*

*Copyright 2026 OntarioMD. This document is not for distribution and should not be construed as legal advice*