

PITO Privacy & Security Check List

* Denotes mandatory “yes” answers

A. Clinic Policies and Procedures

Y N

1. Do you have an office privacy policy that deals with confidentiality of personal health information including printing, transfer, storage and secure disposal of patient records? *
2. Do you have an audit schedule and procedures in place for a designated individual to routinely and periodically (i.e., spot-audits) monitor audit trails?
3. Are procedures in place for dealing with actual and suspected privacy and security incidents and breach investigations? *
4. Are processes in place to securely dispose of disused devices (storage, computers) that may contain confidential data? *

B. Staff

5. Have you appointed an individual (and delegate) responsible for privacy and security? This person would be responsible for answering questions (e.g. from patients), but also responding to complaints, incidents, breaches, audits and making sure that staff are trained and policies/procedures are up to date. *
6. Have you appointed an individual responsible for ongoing EMR user account management (new user set up, changes to user privileges, de-activation of old user accounts)? *
7. Have staff members signed a confidentiality agreement? *
8. Have staff members been trained about privacy, the BC Personal Information Protection Act (PIPA), and how to confidentially manage personal health information? *
9. Do you have ongoing annual privacy and security awareness training that includes how users must safeguard their userids and passwords, keys, tokens and other access credentials (e.g., do not share passwords)?

C. Partners

10. Do contracts with third parties (e.g. paper shredding service) include privacy and confidentiality clauses? *

D. Patients

- 11. Is a patient privacy notice or other communication materials that inform patient about privacy and information practices, available? *
- 12. Are procedures available for dealing with patient requests for information, corrections, and complaints? *
- 13. Do you have procedures and protocols in place for how to handle patient requests for disclosure directives (masking)?

E. EMR Set-up and Configuration – *To be answered by EMR Vendor*

- 14. Has a unique user ID and password been assigned to each individual user accessing the EMR? *
- 15. Have you developed and implemented a roles-based access model? *
- 16. Has the systems audit trail functionality been enabled? *

F. Hardware and peripherals – *To be answered by EMR Vendor*

- 17. Are peripheral devices (printers, fax machines) located in secure areas to prevent unauthorized access? *
- 18. Are computer monitors situated in a manner that prevents unauthorized viewing? *
- 19. Is any patient data stored on desktop computers, laptops, or mobile storage (e.g. memory keys) encrypted? *
- 20. Are procedures and technical controls, e.g. application time-out, in place to prevent screens from being viewed if the computer user leaves the computer? (Time-out specification is up to the practice) *
- 21. Has up-to-date antivirus protection been installed on workstations? *
- 22. Are firewalls installed on computers? *
- 23. Are anti-virus controls always 'on' and enabled? *

G. Local Area Network – *To be answered by Clinic Technical resource*

- 24. Have appropriate controls been set up to secure the local area network (LAN)? *
- 25. Have wireless security settings been appropriately configured and enabled (e.g., restrict wireless transmission, encryption is used, etc.)? *

Privacy & Security Checklist Practice Sign-off

Signature: _____

Date: _____

month/day/year

Name:

Role:

Received by PITO

Signature: _____

Date: _____

month/day/year

Name:

Role: PITO Local Relationship Manager