

PITO Privacy & Security Check List

A. Clinic Policies and Procedures	<u>Y</u>	<u>N</u>	<u>Comments</u>
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?	<input type="checkbox"/> *	<input type="checkbox"/>	
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?	<input type="checkbox"/>	<input type="checkbox"/>	
3. Are procedures in place for dealing with actual and suspected privacy and security incidents and breach investigations?	<input type="checkbox"/> *	<input type="checkbox"/>	
4. Are processes in place to securely dispose of old devices (storage, computers) that may contain confidential data?	<input type="checkbox"/> *	<input type="checkbox"/>	
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.	<input type="checkbox"/> *	<input type="checkbox"/>	
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)?	<input type="checkbox"/> *	<input type="checkbox"/>	
7. Have staff members signed a confidentiality agreement?	<input type="checkbox"/> *	<input type="checkbox"/>	
8. Have staff members been trained about how to maintain privacy and confidentiality of personal health information?	<input type="checkbox"/> *	<input type="checkbox"/>	
9. Do you have ongoing annual privacy and security awareness training that includes how users must safeguard their user IDs and passwords, keys, tokens and other access credentials?	<input type="checkbox"/>	<input type="checkbox"/>	
C. Partners			
10. Do contracts with third parties (e.g. paper shredding service) include privacy and confidentiality clauses?	<input type="checkbox"/>	<input type="checkbox"/>	

* Denotes a mandatory "yes" answer

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? *

E. EMR Set-up and Configuration

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

F. Hardware and peripherals

- 16. Are peripheral devices (printers, fax machines) located in secure areas to prevent unauthorized access? *
- 17. Are computer monitors situated in a manner that prevents unauthorized viewing? *
- 18. Is any patient data stored on desktop computers, laptops, or mobile storage (e.g. memory keys) encrypted? *
- 19. 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? *
- 20. Has up-to-date antivirus protection been installed on workstations? *
- 21. Are firewalls installed on computers? *
- 22. Are anti-virus controls always 'on' and enabled? *

G. Local Area Network

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

* Denotes a mandatory "yes" answer

Privacy & Security Checklist Practice Sign-off

Clinic Name: _____

Signature: _____

Date: _____
month/day/year

Name:

Role:

Received by PITO

Signature: _____

Date: _____
month/day/year

Name:

Role: