Physician Office Security – Safeguards 101
Clinic IT Security Self-Assessment

Use the knowledge you gained in the *"Physician Office Security – Safeguards 101"* workshop to reflect on how your clinic manages information privacy and security. Performed regularly and after each incident, this self-assessment ensures the implemented safeguards are effective and helps to build a security culture.

For updates and new resources, visit the Security Section on the Doctors Technology Office website.

Administrative Safeguards

SAFEGUARD	YES	NO	NOT SURE	COMMENTS/QUESTIONS
1. My clinic has a designated Privacy Officer	☐	☐	☐	
2. My clinic has a designated Security Lead	☐	☐	☐	
3. The Privacy Officer and Security Lead have clear and documented responsibilities	☐	☐	☐	
4. My clinic has documented privacy and security policies and procedures	☐	☐	☐	
5. Current privacy and security policies are available to all staff and external parties who have access to the clinic's computer system.	☐	☐	☐	
6. My clinic team participates in regular training regarding privacy and security requirements.	☐	☐	☐	
7. Our clinic regularly discusses privacy and security topics and concerns that may impact patient information security	☐	☐	☐	
8. Our clinic has a Privacy & Security Binder to house our resources, onboarding materials, and track staff training.	☐	☐	☐	
9. Staff at my clinic are required to sign confidentiality agreements that are filed as part of the record keeping.	☐	☐	☐	
10. My clinic team is aware of malicious emails and have been informed not to click links or open attachments that appear suspicious.	☐	☐	☐	
11. My staff are aware that passwords must be strong, unique, and not shared or re-used for other services (e.g. Gmail, Facebook, LinkedIn).	☐	☐	☐	

SAFEGUARD	YES	NO	NOT SURE	COMMENTS/QUESTIONS
12. Staff are not provided computer access with Administrative Rights	☐	☐	☐	
13. My clinic retains detailed records/receipts for technical services provided by vendors and local IT staff for at least 2 years.	☐	☐	☐	

Physical Safeguards

SAFEGUARD	YES	NO	NOT SURE	COMMENTS/QUESTIONS
14. The clinic site is protected by monitored alarm and fire suppression systems.	☐	☐	☐	
15. Computers are properly positioned so unauthorized individuals cannot see personal information on these screens.	☐	☐	☐	
16. Areas used for storing personal information is restricted to authorized personnel.	☐	☐	☐	
17. Hard copy records containing personal information are securely destroyed.	☐	☐	☐	

Technology Safeguards

SAFEGUARD	YES	NO	NOT SURE	COMMENTS/QUESTIONS
18. My staff is aware that the "Save password" feature in browsers are not used when accessing applications and systems via internet.	☐	☐	☐	
19. The software and hardware is up to date in my clinic.	☐	☐	☐	
20. Patient and the public cannot access my wireless and wired network.	☐	☐	☐	
21. Personal information is not stored on obsolete electronic equipment or computers.	☐	☐	☐	
22. There is a backup process for the secure storage of data in our clinic.	☐	☐	☐	