Clinic Security Self-Assessment checklist

|  |  |
| --- | --- |
| Date Performed: |  |

Perform your clinic assessment regularly and after each incident to ensure security is adequate and implemented safeguards are effective.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ADMINISTRATIVE SAFEGUARD | Yes | No | Unsure | Comments |
|  |  |  |  |  |
| 1. My clinic has a designated Privacy Officer
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic has a designated Security Lead
 | 🞏 | 🞏 | 🞏 |  |
| 1. The Privacy Officer and Security Lead have clear and documented responsibilities
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic has documented privacy and security policies and procedures
 | 🞏 | 🞏 | 🞏 |  |
| 1. Current privacy and security policies are available to all staff and external parties who have access to the clinic’s computer system.
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic team participates in regular training regarding privacy and security requirements.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Our clinic regularly discusses privacy and security topics and concerns that may impact patient information security
 | 🞏 | 🞏 | 🞏 |  |
| 1. Our clinic has a Privacy & Security Binder to house our resources, onboarding materials, and track staff training.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Staff at my clinic are required to sign confidentiality agreements that are filed as part of the record keeping.
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic team is aware of malicious emails and have been informed not to click links or open attachments that appear suspicious.
 | 🞏 | 🞏 | 🞏 |  |
| 1. My staff are aware that passwords must be strong, unique, and not shared or re-used for other services (e.g. Gmail, Facebook, LinkedIn).
 | 🞏 | 🞏 | 🞏 |  |
| 1. Staff are not provided computer access with administrative rights.
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic retains detailed records/receipts for technical services provided by vendors and local IT staff for at least 2 years.
 | 🞏 | 🞏 | 🞏 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PHYSICAL SAFEGUARD | Yes | No | Unsure | Comments |
|  |  |  |  |  |
| 1. The clinic site is protected by monitored alarm and fire suppression systems.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Computers are properly positioned so unauthorized individuals cannot see personal information on these screens.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Access to servers and other network equipment is restricted and protected from fire and water damage.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Areas used for storing personal information is restricted to authorized personnel.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Hard copy records containing personal information are securely destroyed.
 | 🞏 | 🞏 | 🞏 |   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TECHNOLGY SAFEGUARD | Yes | No | Unsure | Comments |
| j |  |  |  |  |
| 1. Staff is aware that the “Save Password” feature in browsers should not be used when accessing applications and systems via internet.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Staff is aware of the risks associated with USB drives and other portable devices that might compromise my network.
 | 🞏 | 🞏 | 🞏 |  |
| 1. My clinic maintains inventory of electronic devices and inventory of software versions.
 | 🞏 | 🞏 | 🞏 |  |
| 1. The software and hardware is up to date in my clinic.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Patient and the public cannot access my wireless and wired network.
 | 🞏 | 🞏 | 🞏 |  |
| 1. Personal information is not stored on obsolete electronic equipment or computers.
 | 🞏 | 🞏 | 🞏 |  |
| 1. There is a backup process for the secure storage of information in my clinic.
 | 🞏 | 🞏 | 🞏 |  |