Privacy and Security Safeguard Checklist

Physical Safeguards

Records, both on-site and off-site, are held and stored in an organized, safe and secure manner.	☐ Yes ☐ No
Rooms and/or cabinets used to store health information are locked when not in use.	☐ Yes ☐ No
Record storage areas are equipped with smoke detectors, fire extinguishers and sprinkler systems when possible.	☐ Yes ☐ No
The distribution of keys is strictly controlled and keys are returned by staff after their employment has been terminated.	☐ Yes ☐ No
Building premises are protected by building alarms. Alarm codes are changed as deemed necessary by the custodian, and past employee codes are deleted.	☐ Yes ☐ No
Health information is not left unattended in areas to which the public has access.	☐ Yes ☐ No
Computer monitors are positioned so that information on the screen cannot be viewed by others in the clinic.	☐ Yes ☐ No
Any electronic system's network server is located in a locked area.	☐ Yes ☐ No
When health information is transported to another location, it is placed in a sealed envelope, marked as confidential and directed to the attention of the authorized recipient.	☐ Yes ☐ No
Staff verifies the identity of courier services used for the transportation of health information.	☐ Yes ☐ No
Fax machines are located in a secure area.	☐ Yes ☐ No
Pre-programmed numbers are used to send fax transmissions and are reviewed at regular intervals to ensure they remain accurate.	☐ Yes ☐ No
All fax transmissions are sent with a cover sheet that indicates the information being sent is confidential and requesting that the information be returned to the clinic if sent to the wrong number.	☐ Yes ☐ No
Reasonable steps are taken to confirm that health information transmitted via fax is sent to a secure fax machine and to confirm that the information was received.	☐ Yes ☐ No
Health information in paper format is disposed of by confidential shredding.	☐ Yes ☐ No
Destruction is documented by listing the records/files to be destroyed, recording the date of destruction and having a staff member sign off that the destruction occurred.	☐ Yes ☐ No
All information is wiped clean with an appropriate disk wiping utility before disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CDROMS) or the device(s) and storage medium be physically destroyed.	☐ Yes ☐ No

Administrative Safeguards

Privacy and security policies and procedures have been developed and are updated as necessary and reviewed regularly (Suggestion: review and update yearly).	☐ Yes ☐ No
Only the least amount of information necessary for the intended purpose is collected, used and disclosed by all physicians and employees.	☐ Yes ☐ No
Access to health information is restricted to only staff who require access to health information to perform their job duties.	☐ Yes ☐ No
Confidentiality and security of health information are addressed as part of the conditions of employment for new staff and is written into job description and contracts.	☐ Yes ☐ No
Staff are monitored for compliance with policies and procedures.	☐ Yes ☐ No
All new staff are required to review policies and procedures, and sign off that they have read, understood and will abide by them.	☐ Yes ☐ No
All staff are required to attend HIA, and related privacy and security, training sessions (Suggestion: provide regular updates at staff meetings and search for AMA's Privacy Training).	☐ Yes ☐ No
All staff, students, volunteers and contracted personnel (e.g. janitors, temporary staff, etc.) are required to sign an Oath of Confidentiality (available in the AMA Resource Centre).	☐ Yes ☐ No
Upon termination of employees or third parties (e.g. software vendors, consultants, locums, etc.), the following procedures are to be followed:	
a) All sensitive materials are to be retrieved, including access control items like badges, keys, fobs or security tokens, and revocation of the door and access keys and cards.	☐ Yes ☐ No
b) Retrieve all system related documentation including any documents containing health information and ensure all tasks, notes and documents in EMR are reviewed.	☐ Yes ☐ No
c) Terminate all user accounts, passwords and alarm codes.	☐ Yes ☐ No
Before implementing new, or changing existing administrative practice or information system that relates to the collection, use and disclosure of individually identifying health information, a Privacy Impact Asesment (PIA) is completed and submitted to the Office of the Information and Privacy Commissioner (OIPC).	☐ Yes ☐ No
Staff know to report all privacy compliance issues, near misses and security breaches to the clinic Privacy Officer.	☐ Yes ☐ No
Health information is retained in accordance with specific records retention provisions as set out by the College of Physicians and Surgeons of Alberta (CPSA) guidelines.	☐ Yes ☐ No

Technical Safeguards

All system users are assigned a unique identifier (user ID) that restricts access to health information and systems that are required for the administration of their job duties (e.g. EMR logins, computer logins, etc.).	☐ Yes ☐ No
Access to electronic systems are password protected.	☐ Yes ☐ No
Passwords are always kept confidential and are not written down, posted publicly or shared with other staff. (Suggestion: Passwords should be at least eight characters long and include at least one number and one symbol (e.g. @#$%^&). Use passphrases, not names that could easily be guessed, like your name, or your pet's' or children's name.)	☐ Yes ☐ No
Passwords are changed every three months.	☐ Yes ☐ No
Computer are locked every time they are unattended, even if for a short time.	☐ Yes ☐ No
Health information sent via email over public or external networks is encrypted.	☐ Yes ☐ No
If a wireless network is implemented, it will be set up according to the requirements established by the custodian. This includes:	
a) The access device (e.g. modem) will be securely fastened on an inside wall of the practice in a non-public access area (e.g. dispensary).	☐ Yes ☐ No
b) Either Wi-Fi Protected Access (WPA) or WPA2 (Wi-Fi Protected Access2) encryption will be used.	☐ Yes ☐ No
c) The default SSID (Service Set Identifier) will be changed, and the SSID broadcast disabled.	☐ Yes ☐ No
d) Default administrator passwords and usernames will be changed to a unique username and strong passphrase. Access to the username and password will be restricted to the custodian and authorized contracted IT support.	☐ Yes ☐ No
e) Firewalls will be enabled for the access device and all computers.	☐ Yes ☐ No
f) Connection to the wireless system will be authorized by the clinic Privacy Officer.	☐ Yes ☐ No
g) If clinics allow patients to access the Wi-Fi, they will set up a public connection that will not be used to connect clinic devices.	
h) Use of any mobile computing devices (e.g. laptops, iPads, USBs, portable hard drives) must be authorized by the lead custodian or privacy officer.	☐ Yes ☐ No
i) The lead custodian will determine what staff are allowed to access via their mobile device (e.g. drug information website).	☐ Yes ☐ No
j) All mobile devices that have the capability should be secured with Alberta Health compliant passwords, PINs or other log-in requirements.	☐ Yes ☐ No
k) Mobile devices should be securely stored in the no-public access area of the clinic when not in use (e.g. locked drawer or cabinet in the dispensary).	☐ Yes ☐ No
l) All devices should be locked in the trunk of the car when transporting them to and from the clinic.	☐ Yes ☐ No
l) An inventory of mobile devices owned by the clinic will be maintained by the clinic privacy officer (e.g. MAC addresses, serial numbers).	☐ Yes ☐ No

Information systems must be capable of creating and maintaining logs of access to patient information. The log should contain the following information:	
a) User identification associated with an access.	☐ Yes ☐ No
b) Role or job function of user.	☐ Yes ☐ No
c) Date and time of an access.	☐ Yes ☐ No
d) Actions performed by the user (e.g. creating, viewing, editing, deleting).	☐ Yes ☐ No
e) Identification of the individual whose record was accessed (e.g. name, personal health number).	☐ Yes ☐ No
Information systems are audited to detect unauthorized access and prevent modification or misuse of health information.	☐ Yes ☐ No
Audit trails are reviewed as deemed necessary by the custodian (at minimum on an annual basis), and anytime there is a privacy incident.	☐ Yes ☐ No
Health information is protected from unauthorized external access by a firewall.	☐ Yes ☐ No
Virus scanning software is installed to protect health information from unauthorized modification, loss, access or disclosure.	☐ Yes ☐ No
Systems are regularly patched with critical patches being applied as soon as possible. (Suggestion: enable automatic updating for operating systems.)	☐ Yes ☐ No
The lead custodian will ensure that software is reviewed on a regular basis and patched as needed. Devices that require patching include servers, computers and mobile devices. Some hardware will require patching as well (e.g., hardware based appliances, like firewalls, routers, SANs, etc.)	☐ Yes ☐ No
Electronic systems are backed up on a daily basis.	☐ Yes ☐ No
Back-up information is stored in a secure, locked environment off-site. External back-up drives (physical devices) should be stored in a secure locked environment off-site. Data backed up by third parties (cloud-based) should remain in Canada.	☐ Yes ☐ No
Information intended for long-term storage on electronic media is reviewed on an annual basis to ensure the data is retrievable and to migrate the data to another storage medium if necessary.	☐ Yes ☐ No
The custodian is responsible for authorizing and approving all software installations and alterations. Installed software is periodically reviewed and unneeded software is removed from the system.	☐ Yes ☐ No