Privacy & Security Risk Assessment

Search AMA's Resource Centre for any of the Suggested Resources listed in this document.

Part A. Physical Environment Risks & Physical Safeguards

Name: ____________________ **Date:** ____________

	Privacy Risk	Safeguard Considerations	Yes	No	Suggested Resources
1	**Errors in information handling and compliance with legislation**	Does the clinic have a process for verifying the identity of patients?	□	□	Collection, use and disclosure policy Notification of Collection of Health Information Poster Information Security in Contracting Policy
		Is there written documentation that identifies the clinic's purpose for collecting health information, authority to collect and who to contact regarding privacy concerns?	□	□	
		Does the clinic have a process for verifying the identity of contractors and their employees, vendors and couriers?	□	□	
2	**Information could be lost and misused**	Are servers, computers, laptops and smartphones with EMR access to patient health information reasonably secured to prevent theft?	□	□	Information Handling Policy
		Are fire extinguishers, smoke detectors, deadbolt locks and other general security items in place?	□	□	
3	**Information could be accessed by people without authority**	Are there policies and procedures in place for securing patient health information?	□	□	Information Handling Policy
		Are there policies and procedures for the retention and secure destruction of health information?	□	□	
		Are patient records in paper format secured away from public access within the clinic?	□	□	
		Are wireless routers stored away from easily accessible areas?	□	□	
		Does the clinic have a list of people with authorized access (e.g., key FOBs, door keys, alarm passcodes, swipe cards) and is it updated regularly?	□	□	

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
		Does each authorized staff member have their own alarm code?	□	□	
		Does the clinic have an intrusion system (e.g., monitoring noise/motion, alarms, automated response, other theft prevention measures)?	□	□	
		Are the clinic locks and alarms regularly tested to ensure they are working properly and are the security company contact lists up to date?	□	□	
4	**Information could be disclosed and misused**	Are strategies used to reduce people overhearing confidential information within the clinic (e.g., radio or television in the waiting room, white noise)?	□	□	Information Handling Policy Fax Transmission Guidelines Email Guidelines
		Are clinic fax machines and printers located in a secure area away from public view and access?	□	□	
		Is a written 'if received in error' notification included on all clinic fax cover sheets and emails?	□	□	

Physical Environment Risks & Physical Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risk #	Safeguards Needed	Action Plan	Responsible	By When

Part B. People Risks & Administrative Safeguards

Name: ____________________ **Date:** ____________

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
1.	**Errors in information handling and compliance with legislation**	Has an individual(s) been designated as the privacy officer?	□	□	Privacy Officer Handbook
		Is there an individual responsible for addressing and responding to patient privacy complaints?	□	□	
		Does the clinic have established and implemented policies and procedures in place for protecting health information as required under the Health Information Act (HIA)?	□	□	Policies and Procedures Table
		Are policies and procedures regularly reviewed and updated?	□	□	
		Do clinic staff members receive regular privacy training including HIA and cybersecurity training?	□	□	AMA privacy training
		Is there a breach management process in place that reflects mandatory breach reporting? Is it reviewed annually?	□	□	Privacy Breach Management Policy
		Is there a process that enables patients to request updates or corrections to health information?	□	□	Correction or Amendment of Health Information Policy
		Is there a process for patients to request access to their health information?	□	□	Right of Access Policy
		Does the clinic maintain a record of disclosures containing all relevant details for each information request?	□	□	Information Handling Policy
		Is written consent obtained from patients when health information is disclosed as outlined in the HIA? (when required)	□	□	Release of Information and Disclosure Process Consent form
		Are there policies and procedures that mandate the safeguarding of health information by all clinic staff?	□	□	Information Handling Policy
		Is there a policy for handling patient information in a consistent manner?	□	□	

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
		Is there an Internet usage policy?	□	□	Information Handling Policy
2.	**Information could be lost and misused**	Is an Information Management Agreement (IMA) in place for any third-party vendor that has access to patient information?	□	□	IMA template
		Do vendors and contractors (e.g., cleaners, maintenance) sign a non-disclosure/confidentiality agreement?	□	□	Information Security in Contracting Policy Non-Disclosure Agreement
3.	**Information could be accessed by people without authority**	Is there a new hire checklist that covers access controls?	□	□	
		Is there a checklist for when employees leave that covers removing access controls and returning equipment?	□	□	
4.	**Information could be disclosed and misused**	Have all affiliates signed an oath of confidentiality and are they updated annually?	□	□	Oath of Confidentiality

People Risks & Administrative Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risk #	Safeguard Needed	Action Plan	Responsible	By When

Part C: Technology Risks & Technical Safeguards

Name: ____________________ **Date:** ____________

Privacy Risk		Safeguards Considerations	Yes	No	Suggested Resources
1	**Errors in information handling and compliance with legislation**	Does the clinic back up non-EMR data such as personnel files and email?	□	□	Information Handling Policy
2	**Information could be accessed by external people without authority**	Does a password-protected screensaver automatically display after the computer has been idle for a reasonable period of time, given where the computer is located in the clinic?	□	□	
		Does everyone lock their computer (e.g., "ctrl-alt-del" key combination) if it's unattended?	□	□	
		Does the EMR automatically log off the user if it has been idle for more than a reasonable period of time?	□	□	
		Is dual authentication required for logging in?	□	□	
		Are computer hard drives set up with encryption?	□	□	
		Is the clinic using a known anti-virus or anti-spyware software? Is the software updated automatically?	□	□	
		Is the computer operating system updated regularly?	□	□	
		Is the wireless network encrypted with tools such as Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2)?	□	□	Wireless Networking and Remote Access Policy Password Guidelines
		Is a secure wireless channel utilized if a clinic laptop is used outside of the clinic?	□	□	
		Is everyone required to change their passwords every 90 days for access to clinic computers, EMR and Alberta Netcare?	□	□	
		Are password standards enforced in the EMR solution and clinic computers?	□	□	

Privacy Risk		Safeguards Considerations	Yes	No	Suggested Resources
		Are there established policies and procedures regarding the transmission of health information via email?	□	□	Email Acceptable Use Guidelines
3	**Information could be accessed by internal people without authority**	Are audit logs completed regularly, reviewed and documented?	□	□	Information Handling Policy
		Is everyone assigned a unique user ID and aware not to share IDs and passwords for EMR access?	□	□	Password Guidelines
		Are staff assigned appropriate user access rights for the EMR and computer network?	□	□	Information Handling Policy

Technology Risks & Technical Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risks #	Safeguard Needed	Action Plan	Responsible	By When