# Privacy & Security Risk Assessment

# Introduction

Privacy and security risk assessments are conducted by clinics to determine if there are gaps in a clinic’s privacy and security policies, practices and procedures. It will help fulfil the custodians’ obligations under the Alberta Health Information Act (HIA) to periodically ensure that proper safeguards for protecting information are in place.

## Objectives

The purpose of the privacy and security risk assessments are to:

* **Enable** a clinic to analyze its privacy and security policies, procedures and practices.
* **Identify** privacy and/or security risks and determine if clinic controls are in place to mitigate those risks.
* **Develop and implement** privacy and security improvements and controls where necessary to reduce clinic privacy and security risks.

## How to Use the Tool

This tool presents a series of risks and questions that will help the clinic determine if key privacy risks are being addressed. The risks are organized under:

* **Physical Environment Risks & Physical Safeguards**
* **People Risks & Administrative Safeguards**
* **Technology Risks & Technical Safeguards**

Guidance about what risk you are assessing and mitigating are provided in each section. This tool will assist you in developing a plan to help ensure that appropriate safeguards are in place. It is recommended that you keep or save the completed tool in a safe place as it provides documentation that the risk assessment was completed and the action plan that was created. This privacy and security risk assessment is intended to be completed on a regular basis (e.g., annually).

 **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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/collection-use-and-disclosure-policy.docx) |
| Is there written documentation that identifies the clinic’s purpose for collecting health information, authority to collect and who to contact regarding privacy concerns?  | ☐ | ☐ | Notification of Collection of Health Information Poster  |
| Does the clinic have a process for verifying the identity of contractors and their employees, vendors and couriers?  | ☐ | ☐ | [Information Security in Contracting Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/info-security-for-contractors-policy.docx) |
| **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?  | ☐ | ☐ |  |
| Are fire extinguishers, smoke detectors, deadbolt locks and other general security items in place?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| **3** | **Information could be accessed by people without authority**  | Are there policies and procedures in place for securing patient health information?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Are there policies and procedures for the retention and secure destruction of health information?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Are patient records in paper format secured away from public access within the clinic?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Are wireless routers stored away from easily accessible areas? | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| 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?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| 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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx)  |
| Are clinic fax machines and printers located in a secure area away from public view and access?  | ☐ | ☐ | [Fax Transmission Guidelines](https://www.albertadoctors.org/About%20the%20AMA_Privacy/facsimile-transmission-policy.docx)[Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is a written ‘if received in error’ notification included on all clinic fax cover sheets and emails?  | ☐ | ☐ | [Email Guidelines](https://www.albertadoctors.org/About%20the%20AMA_Privacy/acceptable-use-of-email-policy.docx)[Fax Transmission Guidelines](https://www.albertadoctors.org/About%20the%20AMA_Privacy/facsimile-transmission-policy.docx) |

**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?  | ☐ | ☐ | Privacy Officer Handbook |
| 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](https://www.albertadoctors.org/clinic-patient-privacy/pia-policies-procedures-table-section-e.docx) |
| 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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/correction-or-amendment-health-info-poli.docx) |
| Is there a process for patients to request access to their health information?  | ☐ | ☐ | [Right of Access Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/access-to-health-info-policy.docx) |
| Does the clinic maintain a record of disclosures containing all relevant details for each information request?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is written consent obtained from patients when health information is disclosed as outlined in the HIA? (when required) | ☐ | ☐ | [Release of Information and Disclosure Process](https://www.albertadoctors.org/About%20the%20AMA_Privacy/collection-use-and-disclosure-policy.docx) [Consent form](https://www.albertadoctors.org/clinic-patient-privacy/disclosure-consent-form.docx) |
| Are there policies and procedures that mandate the safeguarding of health information by all clinic staff?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is there a policy for handling patient information in a consistent manner?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is there an Internet usage policy?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| **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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/info-security-for-contractors-policy.docx)[Non-Disclosure Agreement](https://www.albertadoctors.org/About%20the%20AMA_Privacy/non-disclosure-agreement-tool.docx)  |
| **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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| **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?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Does everyone lock their computer (e.g., “ctrl-alt-del” key combination) if it’s unattended?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Does the EMR automatically log off the user if it has been idle for more than a reasonable period of time?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is dual authentication required for logging in?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Are computer hard drives set up with encryption? | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| Is the clinic using a known anti-virus or anti-spyware software? Is the software updated automatically? | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| 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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/Wireless-networking-and-remote-access-po.docx) |
| Is a secure wireless channel utilized if a clinic laptop is used outside of the clinic?  | ☐ | ☐ | [Wireless Networking and Remote Access Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/Wireless-networking-and-remote-access-po.docx) |
| Is everyone required to change their passwords every 90 days for access to clinic computers, EMR and Alberta Netcare? | ☐ | ☐ | [Wireless Networking and Remote Access Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/Wireless-networking-and-remote-access-po.docx)[Password Guidelines](https://www.albertadoctors.org/clinic-patient-privacy/password-policy-tool.docx) |
| Are password standards enforced in the EMR solution and clinic computers?  | ☐ | ☐ | [Wireless Networking and Remote Access Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/Wireless-networking-and-remote-access-po.docx)[Password Guidelines](https://www.albertadoctors.org/clinic-patient-privacy/password-policy-tool.docx) |
| Are there established policies and procedures regarding the transmission of health information via email? | ☐ | ☐ | [Email Acceptable Use Guidelines](https://www.albertadoctors.org/About%20the%20AMA_Privacy/acceptable-use-of-email-policy.docx) |
| **3** | **Information could be accessed by internal people without authority**  | Are audit logs completed regularly, reviewed and documented?  | ☐ | ☐ | [Information Handling Policy](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |
| 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](https://www.albertadoctors.org/About%20the%20AMA_Privacy/information-handling-policy.docx) |

**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** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |