Commit

**University Research Ethics Board (UREB)**



**REB.FORM.015 | Privacy Breach Report**

|  |
| --- |
| **Introduction:**  This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia and modified for use by Mount Saint Vincent University’s University Research Ethics Board (UREB).  All privacy breaches involving participants in research conducted under the auspices of MSVU must be reported immediately to the UREB using this form. Upon receipt of this form, the UREB will immediately send a copy of the form to the **MSVU FOIPOP** officer for their review and action.  Researchers may use this document in combination with the *Key Steps to Responding to Privacy Breaches* document produced by the OIPC Nova Scotia and available at: <http://foipop.ns.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27.pdf> |

|  |  |
| --- | --- |
| Section A – Ethics File Details | |
| 1. Date | Click or tap to enter a date. |
| 2. Research Ethics Clearance File # | Click or tap here to enter text. |
| 3. Title of Research Study | Click or tap here to enter text. |

|  |  |
| --- | --- |
| Section B – Applicant Information | |
| 1. Principal Investigatoror Nominated Principal Investigator (see REB.INFO.001 for definitions) | Click or tap here to enter text. |
| 2. Department/Faculty | Click or tap here to enter text. |
| 3. Email Address (MSVU email only) | Click or tap here to enter text. |
| 4. Telephone Number | Click or tap here to enter text. |
| 5. Researcher Category | Choose an item.  If you chose Other, please specify:  Click or tap here to enter text. |
| \*Please provide your supervisor’s or MSVU Faculty Sponsor’s information below (if applicable): | |
| 6. Supervisor | Click or tap here to enter text. |
| 7. Supervisor’s Email (MSVU email only) | Click or tap here to enter text. |
| 8. Supervisor’s Telephone Number | Click or tap here to enter text. |
| 9. Have there been any changes in research personnel who interact with participants and/or have access to personal data that have not yet been reported to the UREB? | Yes  No  \*If yes, please complete REB.FORM.014 and submit with this request for renewal. Renewal clearance cannot be provided until the requested change to personnel has been cleared. |

|  |  |
| --- | --- |
| Section C – Research Funding | |
| 1. Research Funding Status | Choose an item. |
| 2. Grantor (select all that apply) | Tri-Council (SSHRC, CIHR, NSERC)  Internal  Other External  (Please specify other grantors): Click or tap here to enter text. |
| 3. Principal Investigator on Funding | Click or tap here to enter text. |
| 4. Grant Number(s) | Click or tap here to enter text. |
| 5. Grant Title (if different from REB file) | Click or tap here to enter text. |
| 6. Funding Period | Start Date: Click or tap to enter a date.  End Date: Click or tap to enter a date. |

|  |  |  |
| --- | --- | --- |
| **Section D - Preliminary Privacy Breach Assessment Report** | | |
| **A. Breach Identification and Containment** | | |
| **Instructions:** Review the preliminary assessment list below. If you answer **Yes** or **Unsure** to any of the questions below, complete the remainder of this assessment report and immediately (same day) forward a copy of this report to the UREB. | | |
| **Preliminary Assessment** | **Yes/No** | **Suggested Containment Strategies** |
| 1. Was there an abuse of access privileges (e.g. unauthorized access or use of records that contain personal information)? | Yes  No  Unsure | 1. Immediately restrict, suspend or revoke access privileges until completion of the investigation. 2. Determine whether personal information was further disclosed to others (verbally or via copies). 3. Attempt to retrieve the documents in question, and document the steps taken. 4. Complete this form and send to the UREB. |
| 1. Was personal information inappropriately disclosed (e.g. improper application of severances (material removed or blacked out), incomplete de-identification)? | Yes  No  Unsure | 1. Attempt to retrieve documents. 2. Determine whether personal information was further disclosed to others (verbally or via copies). 3. Document the steps taken. 4. Complete this form and send to the UREB. |
| 1. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)? | Yes  No  Unsure | 1. Attempt to retrace steps and find the lost document(s). 2. Determine whether personal information was further disclosed to others (verbally or via copies). 3. Document the steps taken. 4. Conduct an inventory of the personal information that was or may have been compromised. 5. Complete this form and send to the UREB. |
| 1. Was personal information stolen (e.g. theft of computer equipment or devices)? | Yes  No  Unsure | 1. Attempt to retrieve the stolen equipment or device. 2. Document the steps taken. 3. Complete this form and send to the UREB.. |
| 1. Was personal information in an unencrypted email sent to the wrong address? | Yes  No  Unsure | 1. Cease transmission of email or correspondence to the incorrect address. 2. Determine whether the email address is incorrect in the system (e.g. programmed incorrectly into the system). 3. Attempt to recall the message. 4. Determine where the email went. 5. Request that the recipient delete all affected email or correspondence, with confirmation via email that this has been done. 6. Determine whether personal information was further disclosed to others (verbally or via copies). 7. Document the steps taken. 8. Complete this form and send to the UREB. |
| 1. Was personal information faxed, mailed or delivered to a wrong address? | Yes  No  Unsure | 1. Determine where the document went. 2. Determine whether the address is incorrect in the system (e.g. programmed incorrectly into system). 3. Request that the recipient return the document(s) if mailed, or request that the fax be destroyed, with confirmation that this has been done. 4. Determine whether personal information was further disclosed to others (verbally or via copies). 5. Document the steps taken. 6. Complete this form and send to the UREB. |
| 1. Did a third party compromise (hack into) a system that contains personal information? | Yes  No  Unsure | 1. Contact security and IT to isolate the affected system, disable the affected system, or disable the user account to permit a complete assessment of the breach and resolve vulnerabilities. 2. Document the steps taken. 3. Complete this form and send to the UREB. |
| 1. Did the sale or disposal of equipment or devices that contain personal information occur without a complete and irreversible purging of the item before its sale or disposal? | Yes  No  Unsure | 1. Contact IT. 2. Document the steps taken. 3. Complete this form and send to the UREB. |
| 1. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g. posting of medical appointments or types of leave, home telephone numbers, slides of PowerPoint presentations that contain personal information)? | Yes  No  Unsure | 1. Remove, move or segregate exposed information or files. 2. Preserve evidence. 3. Determine whether personal information was further disclosed to others (verbally or via copies). 4. Document the steps taken. 5. Complete this form and send to the UREB. |
| 1. Was there an inappropriate collection of personal information? | Yes  No  Unsure | 1. Determine whether personal information was further disclosed to others (verbally or via copies). 2. Complete this form and send to the UREB. |
| 1. Was there an unexpected or unintended use of collected data? Is there a risk for re-identification of an affected individual or another identifiable individual? | Yes  No  Unsure | 1. Determine whether personal information was further disclosed to others (verbally or via copies) 2. Complete this form and send to the UREB. |
| 1. Was there an improper or unauthorized creation of personal information? | Yes  No  Unsure | 1. Complete this form and send to the UREB. |
| 1. Was there an improper or unauthorized retention of personal information? | Yes  No  Unsure | 1. Complete this form and send to the UREB. |
| 1. Remarks/Other:   Click or tap here to enter text. | | |

|  |  |
| --- | --- |
| **Section E - Breach Details** | |
| 1. Date(s) of breach | Click or tap to enter a date. |
| 1. Time of breach | Click or tap here to enter text. |
| 1. Location of breach | Click or tap here to enter text. |
| 1. When and how was the breach discovered? | Click or tap here to enter text. |
| 1. Provide a brief description of the breach (what happened, how it happened) | Click or tap here to enter text. |
| 1. Identify the person whose information was compromised (name and personal record identifiers, if applicable). If information regarding more than one person was compromised, please attach a list | Click or tap here to enter text. |
| 1. Is/are the affected individual(s) aware of the breach? | Yes  No  Whether yes or no, request direction from the FOIPOP Officer or the OIPC. |
| 1. Format of information involved | Electronic records  Paper records  Other (describe)  Click or tap here to enter text. |
| 1. What information was involved (check all that apply) | Medical  Employee  Other (describe)  Click or tap here to enter text. |
| 1. List the immediate containment actions and/or interventions, if any | Click or tap here to enter text. |
| 1. Is there information or evidence to support the allegation of the breach? | Yes  No  If yes, please specify  Click or tap here to enter text. |
| 1. Has your supervisor been notified of the breach? (if applicable) | Yes  No |

|  |  |  |
| --- | --- | --- |
| **Section F - Please name the person(s) directly involved in this breach**  **(e.g. witnesses, investigator, individual who may have caused the breach)**  **Attach a list if necessary.** | | |
| Name  Click or tap here to enter text. | Title/Position  Click or tap here to enter text. | Contact information  Click or tap here to enter text. |
| How was this person involved?  Click or tap here to enter text. | | |
| Name  Click or tap here to enter text. | Title/Position  Click or tap here to enter text. | Contact information  Click or tap here to enter text. |
| 2. How was this person involved?  Click or tap here to enter text. | | |

|  |  |  |
| --- | --- | --- |
| Section G – Signature and Agreement | | |
| My/Our signature(s) below confirms that I/we will ensure that all procedures conducted as part of the project will be conducted in accordance with the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans (TCPS) found online at <http://www.pre.ethics.gc.ca/eng/index/> as well as all relevant MSVU University Research Ethics Board policies and procedures and agree to comply with the policies and procedures outlined therein. | | |
| Signature of Principal Investigator or Nominated Principal Investigator | Name:  Click or tap here to enter text. | Date: Click or tap to enter a date. |
| **Faculty Supervisor or MSVU Sponsor (if required)**  In the case of student research, as Faculty Supervisor, my signature below indicates that I have read and approved the application and proposal, deem the project scientifically valid and worthwhile, and agree to provide continuing and thorough supervision of the student(s). I will ensure that the level of risk inherent to the project is balanced by the level of research experience that the student researcher has. I will provide appropriate oversight to ensure that the research will be conducted in accordance with MSVU UREB's policies/procedures and that it adheres to this cleared protocol and consenting process. | | |
| Signature of Faculty Supervisor | Name of Faculty Supervisor:  Click or tap here to enter text. | Date: Click or tap to enter a date. |

**Submission Process:**

1. Researchers are asked to submit the application electronically only to [ethics@msvu.ca](mailto:ethics@msvu.ca)
2. Please note that recruitment and data collection may not begin until a certificate of Research Ethics Clearance has been issued.
3. Researchers may **only** use letters and/or numbers for file names and refrain from using any special characters (e.g., #; &; etc.).
4. All documents must be clearly labeled and reflect how they are referenced in the application.
5. Note - a **maximum of 2 attachments** are permitted for submission– the application (1) and the combined appendices (2)
6. Application packages shall only be accepted in the form of Word documents (\*.doc or \*.docx) or Portable Document Format (\*.pdf)

For details on specific submission criteria, please see [**Guidance Documents**](https://www.msvu.ca/research-at-the-mount/research-ethics/policies-procedures-guidelines/):

* REB.INFO.401 – Faculty & Staff
* REB.INFO.402 – Graduate Students
* REB.INFO.403 – Undergraduate Students

# **For Office Use Only**

# **Appendix 2: Privacy Breach Checklist**

Use this checklist to evaluate your response to a privacy breach and to decide whether or not to report the breach to the Office of the Information and Privacy Commissioner.[[1]](#footnote-1) For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: [http://foipop.ns.ca](http://foipop.ns.ca/).

|  |  |
| --- | --- |
| Date of report | Click or tap to enter a date. |
| Date breach initially discovered | Click or tap to enter a date. |
| **Contact information** | |
| Public Body/Health Custodian/Municipality | Click or tap here to enter text. |
| Contact Person (Report Author) | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Phone | Click or tap here to enter text. |
| E-Mail | Click or tap here to enter text. |
| Mailing Address | Click or tap here to enter text. |
| **Incident Description** | |
| Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?  Click or tap here to enter text. | |

|  |
| --- |
| **Steps 1 & 2: Containment & Risk Evaluation** |

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary.

|  |  |
| --- | --- |
| **Containment**  **Check all of the factors that apply** | |
|  | The personal information has been recovered and all copies are now in our custody and control. |
|  | We have confirmation that no copies have been made. |
|  | We have confirmation that the personal information has been destroyed. |
|  | We believe (but do not have confirmation) that the personal information has been destroyed. |
|  | The personal information is encrypted. |
|  | The personal information is not encrypted. |
|  | Evidence gathered so far suggests that the incident was likely a result of a systemic problem. |
|  | Evidence gathered so far suggests that the incident was likely an isolated incident. |
|  | The personal information has not been recovered but the following containment steps have been taken (check all that apply)  The immediate neighbourhood around the theft has been thoroughly searched.  Used item websites are being monitored but the item has not appeared so far.  Pawn shops are being monitored.  A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received.  A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.  Our audit confirms that no one has accessed the content of the portable storage device.  We do not have an audit that confirms that no one has accessed the content of the portable storage device.  All passwords and system user names have been changed. |
| Describe any other containment strategies used  Click or tap here to enter text. | |

**Nature of Personal Information Involved**

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

|  |  |
| --- | --- |
|  | Name |
|  | Address |
|  | Date of birth |
|  | Government ID number (specify)  Click or tap here to enter text. |
|  | SIN |
|  | Financial information |
|  | Medical information |
|  | Personal characteristics such as race, religion, sexual orientation |
|  | Other (describe)  Click or tap here to enter text. |

**Relationship**

What is the relationship between the recipient of the information and the individuals affected by the breach?

|  |  |
| --- | --- |
|  | Stranger |
|  | Friend |
|  | Neighbour |
|  | Ex-partner |
|  | Co-worker |
|  | Unknown |
|  | Other (describe) |

**Cause of the Breach**

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

|  |  |
| --- | --- |
|  | Accident or oversight |
|  | Technical error |
|  | Intentional theft or wrongdoing |
|  | Unauthorized browsing |
|  | Unknown |
|  | Other (describe)  Click or tap here to enter text. |

**Scope of the Breach**

How many people were affected by the breach?

|  |  |
| --- | --- |
|  | Very few (less than 10) |
|  | Identified and limited group (>10 and <50) |
|  | Large number of individuals affected (>50) |
|  | Numbers are not known |

**Foreseeable Harm**

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to the public body and other individuals if notifications do not occur:

|  |  |
| --- | --- |
|  | **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver’s license numbers, debit card information) |
|  | **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment) |
|  | **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records) |
|  | **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual) |
|  | **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach) |
|  | **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users) |
|  | **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority) |
|  | **Other** (specify)  Click or tap here to enter text. |

**Other Factors**

The nature of the public body’s relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

|  |  |
| --- | --- |
|  | Client/customer/patient |
|  | Research Participant |
|  | Employee |
|  | Student or volunteer |
|  | Other (describe)  Click or tap here to enter text. |

**Risk Evaluation Summary:**

For each of the factors reviewed above, determine the risk rating.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Factor** | **Risk Rating** | | |
| Low | Medium | High |
| 1. Containment |  |  |  |
| 1. Nature of the personal information |  |  |  |
| 1. Relationship |  |  |  |
| 1. Cause of the breach |  |  |  |
| 1. Scope of the breach |  |  |  |
| 1. Foreseeable harm from the breach |  |  |  |
| 1. Other factors |  |  |  |
| **Overall Risk Rating** |  |  |  |

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general, though, a medium or high risk rating will always result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

|  |
| --- |
| **Step 3: Notification** |

**Should affected Individuals be Notified?**

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur. If the *PHIA* test is satisfied, notification must occur.

|  |  |  |
| --- | --- | --- |
| **Consideration** | **Description** | **Factor applies** |
| **Legislation** | Health custodians in Nova Scotia must comply with sections 69 & 70 of *PHIA* which require notification. |  |
| **Risk of identity theft** | Most likely when the breach includes loss of SIN, credit card number, driver’s license number, debit card information, etc. |  |
| **Risk of physical harm** | When the information places any individual at risk of physical harm from stalking or harassment. |  |
| **Risk of hurt, humiliation, damage to reputation** | Often associated with the loss of information such as mental health records, medical records or disciplinary records. |  |
| **Loss of business or employment opportunities** | Where the breach could affect the business reputation of an individual. |  |
| **Explanation required** | The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low. |  |
| **Reputation of public body** | Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low. |  |

**When and How to Notify**

**When:** Notification should occur as soon as possible following a breach. However, if you have contacted law-enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

**How:** The preferred method is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

|  |  |
| --- | --- |
| **Considerations Favouring Direct Notification** | **Check If Applicable** |
| The identities of individuals are known |  |
| Current contact information for the affected individuals is available |  |
| Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach |  |
| Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.) |  |
| **Considerations Favouring Indirect Notification** |  |
| A very large number of individuals are affected by the breach, such that direct notification could be impractical |  |
| Direct notification could compound the harm to the individuals resulting from the breach |  |

**What to Include in Breach Notification Letters**

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

|  |  |
| --- | --- |
| **Essential Elements in Breach Notification Letters** | **Included** |
| Date of breach |  |
| Description of breach |  |
| Description of personal information affected |  |
| Steps taken so far to control or reduce harm (containment) |  |
| Future steps planned to prevent further privacy breaches |  |
| Steps individuals can take - consider offering credit monitoring where appropriate |  |
| Information and Privacy Commissioner’s contact information – Individuals have a right to complain to the Information and Privacy Commissioner |  |
| Public body, municipality or health custodian contact information – for further assistance |  |

**Others to Contact**

|  |  |  |
| --- | --- | --- |
| **Authority or Organization** | **Reason for Contact** | **Applicable** |
| Law-enforcement | If theft or crime is suspected |  |
| Information and Privacy Commissioner for Nova Scotia | * For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation * The personal information is sensitive * There is a risk of identity theft or other significant harm * A large number of people are affected * The information has not been fully recovered * The breach is a result of a systemic problem or a similar breach has occurred before |  |
| Professional or regulatory bodies | If professional or regulatory standards require notification of the regulatory or professional body |  |
| Insurers | Where required in accordance with an insurance policy |  |
| Technology suppliers | If the breach was due to a technical failure and a recall or technical fix is required |  |

**Confirm notifications completed**

|  |  |
| --- | --- |
| **Key contact** | **Notified** |
| Privacy officer within your public body, municipality or health custodian |  |
| Police (as required) |  |
| Affected individuals |  |
| Information and Privacy Commissioner for Nova Scotia |  |
| Professional or regulatory body – identify  Click or tap here to enter text. |  |
| Technology suppliers |  |
| Others (list below)  Click or tap here to enter text. |  |

|  |
| --- |
| **Step 4: Prevention** |

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,[[2]](#footnote-2) and assess if any further adjustments are necessary as part of your prevention strategy.

**Physical Controls**

What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

**Technical Controls**

Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

**Administrative Controls**

Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution’s policies, directives and processes for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

**Personnel Security Controls**

Personnel security controls refer to a public body’s (or health custodian’s) management of its employees – suitability, proper training, supervision and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?

1. The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by l at [oipcns@novascotia.ca](mailto:oipcns@novascotia.ca). [↑](#footnote-ref-1)
2. For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner website at: <http://foipop.ns.ca>. [↑](#footnote-ref-2)