Policy Procedures– Privacy Breach Management

The Multiple Sclerosis Society of Canada ("MS Society") is committed to protecting the personal information under its control and to respecting the privacy of people affected by MS, members, event participants, donors, volunteers, and staff regarding personal information that is collected, used, disclosed and retained by the MS Society of Canada.

While protection is paramount – as outlined in our Privacy and Confidentiality Policy and related procedures – the MS Society recognizes that breaches can occur. To this end, this document outlines the actions to be undertaken by MS Society staff and volunteers in case of a privacy breach.

What is a privacy breach?

A privacy breach is the unauthorized access to or collection, use or disclosure of personal or health information held by the MS Society about individuals who participate in MS Society programs and events, beneficiaries of services, donors, staff or volunteers. Such activity is "unauthorized" if it occurs in contravention to our Privacy and Confidentiality Policy (which is compliant with PIPEDA and similar provincial legislation).

Some of the most common privacy breaches happen when personal information in the custody of the MS Society is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal or health information is stolen, personal information is mistakenly emailed to the wrong person, and the sharing of names and contact information of donors with another organization without their permission.

OBJECTIVES

This document provides staff and volunteers with guidance when a privacy breach occurs. It outlines the steps that need to be taken to determine if a breach has indeed occurred and, if this is the case, respond and contain the breach, notify those affected, and document, investigate and implement change to prevent future breaches.

AUTHORIZATION

These procedures were approved by the Executive Team on October 28, 2015.

PROCEDURES

The MS Society shall investigate all complaints concerning a breach of privacy. If a privacy breach occurs, the MS Society shall assess the situation and implement an appropriate action plan in a timely manner.

Any staff or volunteer that becomes aware of a privacy breach or of the possibility of a privacy breach must take immediate action as outlined below.

The MS Society extends whistleblower protection to any employee or volunteer who reports a breach or a potential contravention of the MS Society's Privacy Policy or of applicable legislation. (See details at Leadership Volunteer and Employee Disclosure and Protection Policy). This protection also extends to those who refuse to perform a transaction that they believe to be in contravention of applicable legislation or the MS Society's Privacy Policy.

The five steps to manage a privacy breach are:

1. Report the breach or suspected breach,
2. Contain the breach,
3. Evaluate the risk associated with the breach,
4. Notify affected individuals,
5. Document, investigate and implement change.

STEP 1: Report the breach or suspected breach

1.1 Notify of possible breach

Any individual working on behalf of the MS Society who becomes aware of a privacy breach or a suspected privacy breach involving personal or health information in the custody or control of the MS Society will immediately inform their immediate supervisor, the division privacy officer and the national privacy officer. (Please refer to ***Appendix B*** for contact information).

When there is a potential conflict of interest or for other reasons, in the interest of confidentiality and as per the Leadership Volunteer and Employee Disclosure and Protection policy and procedures, such reports may be made to another individual in the list below.

- Division president;
- President and chief executive officer;
- External disclosure hotline: 1-866-921-6714 (Whistleblower hotline)

The following information is required when reporting the breach:

- What happened,
- In which department,
- When the incident occurred,

- How and when the incident was discovered,
- Type of data breached, number of people affected by the breach, and
- Whether any corrective action has already been taken.

The division privacy officer will inform the national privacy officer (PO) and the Division President, and will verify the circumstances of the possible breach. The incident will be documented in a privacy incident database.

1.2 Determine if a breach has occurred

The division PO will assess the situation and determine if a breach has occurred. The division PO will engage the national PO in the process.

To determine if a breach has occurred, two questions are critical to answer:

1. **Is personal information involved?** Identify the type of information affected by the incident in order to determine if a breach has occurred. Personal information is recorded information about an identifiable individual and includes, but is not limited to: race, nationality, religion, age, marital status, education, medical (such as MS diagnosis), financial information, address, telephone number, opinions, etc.
2. **Has an unauthorized disclosure occurred?** Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.

If the answer is yes to both questions, a privacy breach has occurred. The division PO needs to follow the rest of the privacy breach response protocol outlined below.

1.3 If a breach has occurred

As soon as the breach has been confirmed to have occurred, the division PO will inform the following:

- Person reporting the breach/possible breach
- National privacy officer
- Assistant Vice-President, Marketing and Communications
- VP Information Technology
- Division President (for regional incidents)
- Chief Executive Officer (for national incidents)
- Chief Financial Officer (who will notify the MS Society insurance provider)

The national PO will notify the Executive Team and keep them updated.

This confirmation needs to occur within 24 hours of the initial report.

1.4 Assemble privacy breach team

When a breach has been confirmed the national PO will assemble a privacy breach team to respond to the incident as soon as reasonably possible and will lead the implementation of the remaining steps of the breach incident protocol.

In addition to the national and division POs, privacy breach team members may include an information security lead, the individual who discovered the breach, a representative from the Marketing and Communications team, senior management, and other members appropriate to the situation. Staff may be asked to assist the team in fulfilling its responsibilities.

The names and contact information for privacy officers and other key individuals to be engaged in case of a privacy breach are listed in ***Appendix B***.

STEP 2: Contain the breach

When a breach of privacy has occurred, the following steps are to be followed. Some steps may be executed concurrently (i.e., notification and containment).

The person who discovers the breach with support from the division PO and other relevant individuals will immediately contain the breach in order to prevent further release of information (e.g. stop the un-authorized practice, recover records, shut down the system that was breached, revoke or change computer access codes, correct weaknesses in security, etc.). Containment should occur simultaneously with notification (e.g., if a fax has gone to the wrong number, contact the recipient and ask that it not be read but shredded with an email to confirm). Containment includes:

- Retrieve as much of the breached information as possible (ideally all);
- Destroy all copies of information that were collected without authorization;
- Ensure no copies of the confidential information have been made or retained by the individual who was not authorized to receive the information; obtain the individual's contact information in the event that follow-up is required;
- Ensure that further breaches cannot occur through the same means at this time.

The privacy breach team will work to determine if the breach would allow unauthorized access to any other personal information / personal health information (e.g., an electronic information system) and take necessary action (e.g., change passwords, identification numbers, and/or temporarily shut down a system).

In consultation with the MS Society's legal counsel and the Chief Executive Officer, the national PO shall notify the police if the breach involves or may involve any criminal activity.

Refer to **Appendix A** for a quick overview of the privacy incident notification process.

STEP 3: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, the privacy breach team will assess the risks associated with the breach. The following factors need to be considered:

- **Personal Information Involved**
  - What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Health information and financial information that could be used for identity theft are examples of sensitive personal information.
  - What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?

- **Cause and Extent of the Breach**
  - What is the cause of the breach?
  - Is there a risk of ongoing or further exposure of the information?
  - What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
  - Is the information encrypted or otherwise not readily accessible?
  - What steps have already been taken to minimize the harm?

- **Individuals Affected by the Breach**
  - How many individuals are affected by the breach?
  - Who was affected by the breach: participants in MS Society programs, events and services, donors, volunteers, staff, service providers, other organizations?

- **Foreseeable Harm From the Breach**
  - Is there any relationship between the unauthorized recipients and the data subject?
  - What harm to the individuals will result from the breach? Harm may include: security risk (e.g. physical safety), identity theft or fraud, loss of business or employment opportunities, and hurt, humiliation, damage to reputation or relationships.
  - What harm could result to the MS Society as a result of the breach? (e.g. loss of trust in the organization, loss of assets, and financial exposure.)

If the risk is determined to significantly impact the reputation of the MS Society, consideration will be given by the Assistant Vice-president, Marketing and Communications or other key individuals to activating the crisis communication plan.

If the information technology security risk is medium or high, consideration will be given by the Vice-president, Information Technology to activate the IT disaster recovery plan.

STEP 4: Notify affected individuals / institutions about the privacy breach

The process of notification depends on the particular breach. The privacy breach team will determine the need for notification using the guidelines below.

4.1 How to determine if notification of individuals / institutions is required

The considerations below will help decide whether affected individuals should be notified. If either of the first two factors listed below applies, notification of the affected individuals must occur. The risk factors that follow are intended to serve as a guide. If none of these applies, no notification may be required. The privacy breach team must use their judgement to evaluate the need for notification of individuals.

Considerations:

1. ***Legislation requires notification***
2. ***Contractual obligations require notification***
3. ***Risk of identity theft***
    - Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with credit card numbers, personal health numbers, or any other information that can be used for fraud by third parties.
4. ***Risk of physical harm***
    - Does the loss of information place any individual at risk of physical harm, stalking, or harassment?
5. ***Risk of hurt, humiliation, damage to reputation***
    - Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as medical records.
6. ***Risk of loss of business or employment opportunities***
    - Could the loss of information result in damage to the reputation of an individual, affecting business or employment opportunities?

Notification should occur as soon as reasonably possible following a breach. However, if law enforcement authorities have been contacted, it should be determined from those authorities whether notification should be delayed so as not to impede a criminal investigation.

4.2 Methods of notification

The preferred method of notification is direct – by phone, in writing or in person – to the affected individuals. The following are considerations favouring **direct notification**:

- The identities of the individuals are known;
- Current contact information for the affected individuals is available;
- Individuals affected by the breach of privacy require detailed information 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.).

Indirect notification – website information, posted notices, advertisements or news releases – should generally be used only 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. The following are 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 individual resulting from the breach.

4.3 What to include in the notification of affected individuals

The privacy breach team shall draft the notification message and will determine under whose signature the notification should be issued.

The purpose of providing notice of a privacy breach to the affected individual(s) is to provide them with sufficient information about:

- What happened and when,
- A generic description of the type(s) of personal information involved in the breach, including whether any unique identifiers of sensitive personal information were involved in the breach,
- The nature of potential or actual risks of harm,
- What action the MS Society has taken to address the situation,
- What appropriate action the individual(s) should take to protect themselves against harm (e.g. tracking credit cards, monitoring bank accounts, how to contact credit reporting agencies, etc.),
- Future steps the MS Society will take to prevent future privacy breaches,
- MS Society contact for further information.

STEP 5: Documentation, Investigation and Remediation

5.1 Documenting the breach

All details of a privacy breach or suspected privacy breach and the containment strategy must be documented. All incidents have to be recorded in the privacy incident database available on the Privacy Officer team site in Mercury.

The privacy breach team will document the following information:

- The nature and scope of privacy breach (e.g. how many people are affected, what type of personal information is involved, the extent to which we have contained the breach) or, if the nature and scope are not known at the time of briefing, that they are still to be determined.
- What steps have already been taken, or will be taking, to manage the privacy breach.
- The plans to notify the individuals affected by the privacy breach, and, if appropriate, other parties.
- If the breach was identified by an external source (e.g. individual, other institution, third party provider), document the information provided, including contact information for follow-ups, and any instructions given to the reporting party (e.g. asking caller to mail back the documents sent to the wrong address).
- The timetable for providing senior management with regular updates about the breach and its ongoing management.

5.2 Investigation and remediation

The national PO with input from privacy breach team will lead an internal investigation to:

- Identify and analyze the events that led to the privacy breach,
- Evaluate what was done to contain it,
- Recommend remedial action to help prevent future breaches. These may include:
    - Review relevant internal processes to ensure compliance with our privacy and confidentiality policy,
    - Amend or reinforce existing policies and practices for managing and safeguarding personal information,
    - Develop and implement new security or privacy measures,
    - Train staff on legislative requirements, security and privacy policies, practices and procedures,
    - Test and evaluate remedial actions to determine if they have been implemented correctly and if policies and practices need to be modified.

MONITORING AND COMPLIANCE

MS Society privacy officers at all levels of the organization are responsible for ensuring compliance with these procedures.

All confirmed privacy breaches must be reported by members of the Executive Team in their quarterly compliance reports to the President and CEO.

RELATED POLICIES, REFERENCES AND LEGISLATION

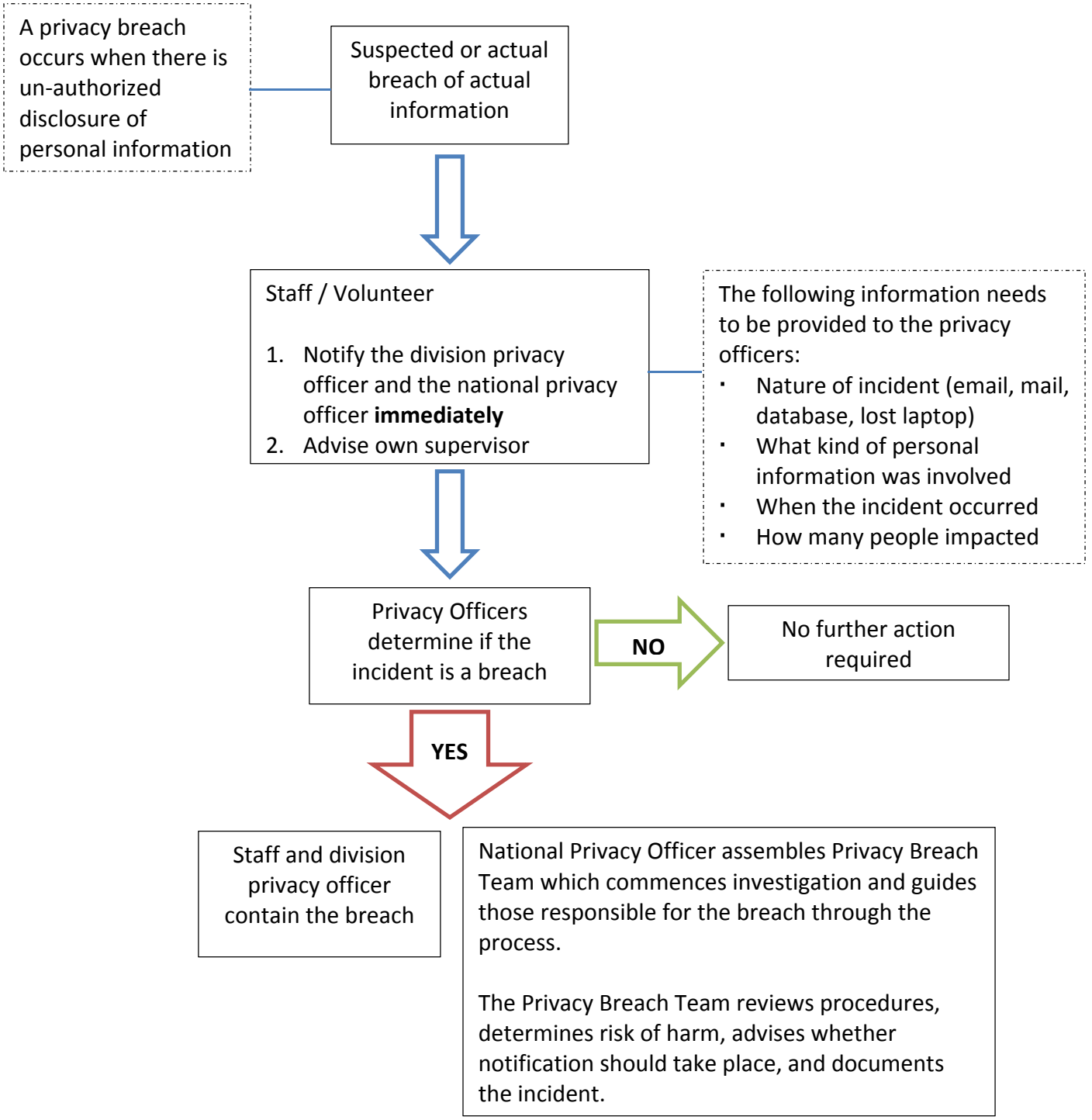
- MS Society Privacy and Confidentiality Policy
- MS Society of Canada – Privacy and You: Privacy and Confidentiality Policy Implementation Procedures
- Leadership Volunteer and Employee Disclosure and Protection Policy
- Leadership Volunteer and Employee Disclosure and Protection (Whistle blower) Procedures

PROCEDURE REVIEW

These procedures are to be reviewed alongside review of its related MS Society of Canada Privacy and Confidentiality Policy every five years.

Appendix A

PRIVACY INCIDENT NOTIFICATION PROCESS



Appendix B

PRIVACY BREACH KEY CONTACT INFORMATION

Privacy officers can be reached at the following email addresses:

National Privacy Officer	priv@mssociety.ca (English) priv@scleroseenplaques.ca (French)
Division Privacy Officers	
Alberta and NWT	priv-alberta@mssociety.ca
Atlantic	priv-atlantic@mssociety.ca
BC and Yukon	priv-bc@mssociety.ca
Manitoba	priv-manitoba@mssociety.ca
Ontario and Nunavut	priv-ontario@mssociety.ca
Quebec	priv-quebec@scleroseenplaques.ca
Saskatchewan	priv-sask@mssociety.ca

The names and contact information for the privacy officers may change from time to time and is available on the Privacy Community of Practice team site here.

Other key positions to be notified in case of a privacy breach:

Assistant Vice-President, Marketing and Communications

Vice-President, Information Technology

Relevant Division President (for regional incidents)

Chief Executive Officer (for national incidents)

Chief Financial Officer

Appendix C

PRIVACY BREACH CHECKLIST

Date of report:	
Date and time breach was initially discovered:	

A. Contact information

Name of person who reported the breach / suspected breach:	
Job title and contact information:	
Name of supervisor (if applicable):	

B. Incident description

Describe the nature of the breach and its cause. How was it discovered and when? Where did it occur?

C. Containment and risk evaluation

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

(1) 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 was encrypted
	The personal information was 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
	The IT department has been notified
	All passwords and system user names have been changed
Describe any other containment strategies used:	

(2) Nature of Personal Information Involved

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

	Name
	Email address
	Address
	Date of birth
	Financial information
	Donor information
	Medical information (i.e. diagnosis of MS)
	Personal characteristics such as race, religion, sexual orientation
	Other (describe)

(3) 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)

(4) 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)

(5) 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

(6) 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 MS Society and other individuals if notifications do not occur:

	Identify theft (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
	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)
	Other (specify)

(7) Other factors

The nature of the relationship between the MS Society and the affected individuals may be such that the MS Society 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.

	Participant in MS Society programs / Recipient of MS Society services
	Donor
	Volunteer
	Employee
	Other (describe)

D. Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating. Please refer to ***Appendix D*** as a guideline for assessment:

Risk Factor	Risk Rating		
	Low	Medium	High
1) Containment			

Risk Factor	Risk Rating		
	Low	Medium	High
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm			
7) Other factors			
Overall Risk Rating			

Use the risk rating in **Appendix D** to help decide whether notification is necessary and design your prevention strategies. Foreseeable harm from the breach is usually a key factor in deciding whether or not to notify affected individuals.

In general, a medium or high risk rating will always result in notification of the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

E. Notification

1) 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.

Consideration	Description	Factor applies
Legislation		
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card 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	

Consideration	Description	Factor applies
Explanation required	The MS Society 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 the MS Society	Where the MS Society is concerned that the breach will undermine trust of stakeholders, it 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	

2) When and How to Notify

When: Notification should occur as soon as possible following a breach. However, if law enforcement authorities were contacted, they should be consulted to determine whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, in writing 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 <u>Direct</u> 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 <u>Indirect</u> 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	

3) 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 by the MS Society to control or reduce harm	
Steps individuals can take to protect themselves	
Future steps planned by the MS Society to prevent further privacy breaches	
MS Society contact information – for further assistance	

4) Others to contact

Authority or Organization	Reason for Contact	Applicable
Law Enforcement	If theft or crime is suspected	
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	
Others (list)		

5) Confirm notifications completed:

Key contact	Notified
Division Privacy Officer	
National Privacy Officer	
Assistant Vice-president Marketing and Communications	
Vice-president, Information Technology	
IT department	
Division President	
Chief Executive Officer	
Chief Financial Officer	
Police (as required)	
Affected individuals	
Legal counsel	
Jurisdictional privacy commissioner	
Others (list)	

Appendix D

PRIVACY RISK RATING OVERVIEW

The table below summarizes the risk factors and suggests a possible risk rating. The table is intended to provide a rough guide to ratings.

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	**Medium**	**High**
Nature of personal information	✓ Publicly available personal information not associated with any other information	✓ Personal information unique to the organization that is not medical or financial information	✓ Medical, psychological, counselling, or financial information or unique government identification number
Relationships	✓ Accidental disclosure to another professional who reported breach and confirmed destruction or return of the information	✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated family members, neighbors or co-workers ✓ Theft by stranger
Cause of breach	✓ Technical error that has been resolved	✓ Accidental loss or disclosure	✓ Intentional breach. ✓ Cause unknown ✓ Technical error – if not resolved
Scope	✓ Very few affected individuals	✓ Identified and limited group of affected individuals	✓ Large group or entire scope of group not identified (over 50)

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	**Medium**	**High**
Containment efforts	✓ Data was adequately encrypted ✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	✓ Data was not encrypted ✓ Data, files or device have not been recovered ✓ Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	✓ No foreseeable harm from the breach	✓ Loss of business or employment opportunities ✓ Hurt, humiliation, damage to reputation or relationships ✓ Social/relational harm ✓ Loss of trust in the MS Society ✓ Loss of MS Society assets ✓ Loss of MS Society contracts or business ✓ Financial exposure to the MS Society including class action lawsuits	✓ Security risk (e.g. physical safety) ✓ Identify theft or fraud risk ✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances ✓ Risk to public health or safety