| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 1 of 23 |
| **Approved:** | | **Revised:** |

## 1.0 POLICY

1.1 As a public body governed by the privacy legislation in British Columbia and Canada, Three Links Care Society ("Three Links") is committed to protecting the personal information under its control and to respecting the privacy of residents, family members, staff, contractors and volunteers regarding personal information that is collected, used, disclosed and retained by Three Links.

1.2 Under the service agreement with Vancouver Coastal Health to provide residential care beds, Three Links is also subject to the Freedom of Information and Privacy Act which sets out the access and privacy rights of individuals as they relate to the public sector.

1.3 While protection is paramount, as outlined in our privacy policies, Three Links recognizes that breaches can occur. To this end, this document provides staff and volunteers with guidance when a privacy breach happens. 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, document, investigate and implement changes to prevent future breaches.

1.4 The Director of Human Resources is the Privacy Officer for Three Links and is responsible for ensuring compliance with the procedures in privacy breach management. In the event the Privacy Officer is unavailable, the Department Manager where the breach occurred will act as the Privacy Officer.

1.5 All confirmed privacy breaches must be reported in the quarterly indicator reports to the Senior Management team and Society Board.

## 2.0 DEFINITIONS

2.1 A "**privacy breach**" is the unauthorized access to or collection, use or disclosure of personal or health information held by Three Links about individuals who reside, work or volunteer at Three Links. Such activity is "unauthorized" if it occurs in contravention to our privacy policies, the

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 2 of 23 |
| **Approved:** | | **Revised:** |

Personal Information Protection and Electronic Documents Act (PIPEDA) and other related government legislation.

Some of the most common privacy breaches occur when personal information in the custody of Three Links 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 residents/staff/volunteers without their permission.

2.2. **"Personal information"** means information about an identifiable individual which may include their personal, financial and health record information.

## 3.0 PROCEDURES

3.1 Three Links will investigate all complaints concerning a breach of privacy. If a privacy breach occurs, Three Links shall assess the situation and implement an appropriate action plan in a timely manner.

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

3.3 Three Links extends whistleblower protection to any employee, contractor or volunteer who reports a breach or a potential contravention of Three Links' privacy policies or applicable legislation. This protection also extends to those who refuse to perform a transaction that they believe to be in contravention of applicable legislation or Three Links' privacy policies.

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 / institutions
5) Document, investigate and implement change

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 3 of 23 | |
| **Approved:** | | **Revised:** | |

## STEP 1 – Report the breach or suspected breach

### 1. Notify of possible breach

Any individual working on behalf of Three Links who becomes aware of a privacy breach or a suspected privacy breach involving personal or health information in the custody or control of Three Links will immediately inform their manager and Privacy Officer.

Where there is a potential conflict of interest or for other reasons, in the interest of confidentiality, such reports may be made to another individual in the list below:

- Director of Care
- Director of Support Services
- Chief Executive Officer

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
- Whether any corrective action has already been taken.

The Privacy Officer will inform the Chief Executive Officer and senior managers, and will verify the circumstances of the possible breach. The incident will be documented in a privacy incident database.

### 2. Determine if a breach has occurred

The Privacy Officer will assess the situation and determine if a breach has occurred.

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 to determine if a breach has occurred. Personal information is recorded information about an identifiable

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 4 of 23 |
| **Approved:** | | **Revised:** |

individual and includes, but is not limited to: race, nationality, religion, age, marital status, education, medical, 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 Privacy Officer needs to follow the rest of the privacy breach response protocol outlined below.

### 3. If a breach has occurred

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

- Person reporting the breach/possible breach
- Director(s) of the affected department(s)
- IT consultant (if the information breached is computerized)
- Chief Executive Officer

### 4. Assemble Risk Management Committee/privacy breach team

When a breach has been confirmed, the Privacy Officer will assemble the Risk Management Committee 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 Privacy Officer and Risk Management Committee, additional members may include an information security lead, the individual who discovered the breach, a communications specialist, senior management and other members appropriate to the situation (the “privacy breach team”). Staff may be asked to assist the team in fulfilling its responsibilities.

## 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 (ie. notification and containment).

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 5 of 23 |
| **Approved:** | | **Revised:** |

1. The person who discovers the breach with support from the Privacy Officer and other relevant individuals will immediately contain the breach to prevent further release of information (eg. stop the unauthorized practice, recover records, shut down the system that was breached, revoke or change computer access codes, correct weakness in security, etc.). Containment should occur simultaneously with notification (eg. 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 copies of information that were collected without authorization;
    - Ensure no copies of 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 (eg. an electronic information system) and take necessary action (eg. change passwords, identification numbers, and/or temporarily shut down a system).

. In consultation with Three Links' legal counsel and the Chief Executive Officer, the Privacy Officer 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**

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 6 of 23 | |
| **Approved:** | | **Revised:** | |

  - 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 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 extend of the unauthorized collection, use of 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: residents, staff, donors, volunteers, 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 (eg. 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 Three Links as a result of the breach? (eg. loss of trust in the organization, loss of assets, and financial exposure)

If the risk is determined to significantly impact the reputation of Three Links, consideration will be given by the Chief Executive Officer or Society Board to initiate a crisis communication plan.

If the information technology security risk is medium or high, consideration will be given by the Chief Executive Officer or Society Board, in consultation with Three Links' IT consultants, to initiate an IT disaster recovery plan.

**STEP 4 – Notify affected individuals / institutions about the privacy breach**

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 7 of 23 | |
| **Approved:** | | **Revised:** | |

The process of notification depends on the particular breach. The privacy breach team will determine the need for notification using the guidelines below. The Privacy Officer will be responsible in notifying the affected parties.

**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 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 3rd 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.

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 8 of 23 |
| **Approved:** | | **Revised:** |

## 2. Methods of notification

The preferred method of notification is direct – by phone, in writing or in person – to the affected individuals. The following 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 individuals resulting from the breach.

## 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

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 9 of 23 |
| **Approved:** | | **Revised:** |

- What appropriate action the individual(s) should take to protect themselves against harm (eg. tracking credit cards, monitoring bank accounts, how to contact credit reporting agencies, etc.)
- Future steps Three Links will take to prevent future privacy breaches
- Three Links contact for further information

## STEP 5 – Documentation, Investigation and Remediation

### 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 by the Privacy Officer.

The privacy breach team will document the following information:

- The nature and scope of privacy breach (eg. 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 (eg. individual, other institution, 3rd party provider), document the information provided, including contact information for follow-ups, and any instructions given to the reporting party (eg. 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.

### 2. Investigation and remediation

The Privacy Officer, with input from the privacy breach team, will lead an internal investigation to:

- Identify and analyze the events that led to the privacy breach

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 10 of 23 | |
| **Approved:** | | **Revised:** | |

- 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
    - Discipline (including legal action) of persons involved in breach if the breach was willful and deliberate by those persons identified during investigation.
    - 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.

**3. Hold a debriefing session to review the breach management procedure**

Once the management and remediation of the breach has concluded and all systems have been put in place, the Privacy Officer will also hold a debriefing session with the privacy breach team to review the breach management procedure for this incident – how the situation was handled, are there any areas in the process that need to be modified, etc. The session will be documented and kept in the privacy breach incident file.

## 4.0 REFERENCES

4.1 HR Policy HRT1000 – Confidentiality

4.2 HR Policy HRT1300 – Employee Privacy

4.3 Admin Policy AE0400 – Confidentiality of Information

4.4 Admin Policy AE0525 – Privacy Policy; Residents

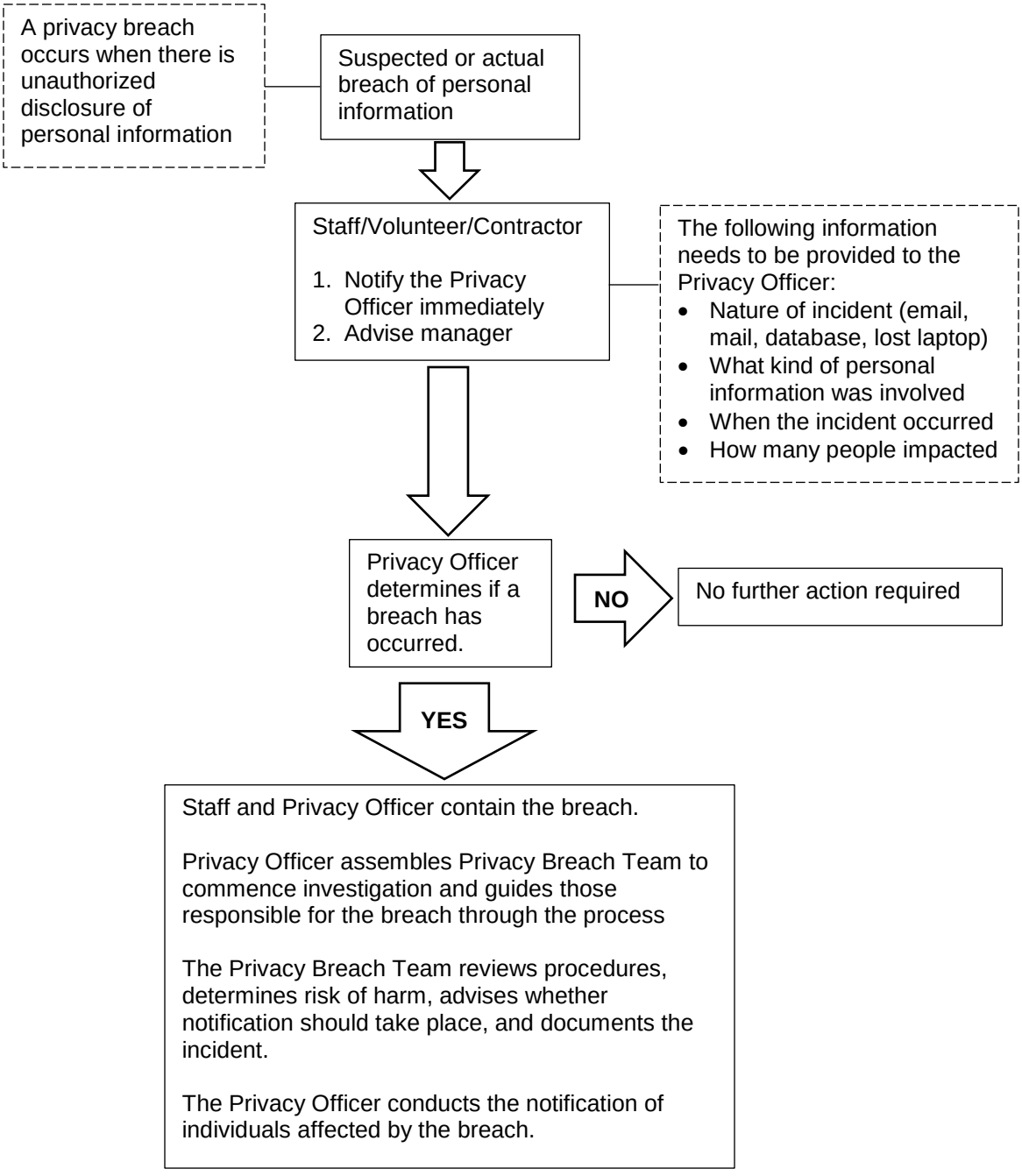
4.5 Personal Information and Privacy Act (PIPA)

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 11 of 23 |
| **Approved:** | | **Revised:** |

4.6 Personal Information Protection and Electronic Documents Act (PIPEDA)

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 12 of 23 | |
| **Approved:** | | **Revised:** | |

## Appendix A – Privacy Incident Notification Process



| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 13 of 23 |
| **Approved:** | | **Revised:** |

**Appendix B**

**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 manager (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**

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 14 of 23 |
| **Approved:** | | **Revised:** |

Check all 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):<br>☐ The immediate neighbourhood has been thoroughly searched<br>☐ The IT department has been notified<br>☐ All passwords and system user names have been changed |
| Describe any other containment strategies used: | |

**(2) Nature of Personal Information Involved**

Check all the data elements involved (eg. name, date of birth, email, address, medical information, etc.):

| | |
|---|---|
| | Name |
| | Email address |
| | Address |
| | Date of birth |
| | Financial Information |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 15 of 23 | |
| **Approved:** | | **Revised:** | |

| | |
|---|---|
| | Donor Information |
| | Medical Information |
| | Personal characteristics such has 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 (between 10 and 50) |
| | Large number of individuals affected (more than 50) |
| | Numbers are not known |

| | | |
|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** |
| **Subject:** | Privacy Breach Management | **Page:** 16 of 23 |
| **Approved:** | | **Revised:** |

**(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 Three Links and other individuals if notifications do not occur.

| | |
|---|---|
| | **Identity 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 medical 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 3rd parties in the case of 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 Three Links and the affected individuals may be such that Three Links 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.

| | |
|---|---|
| | Resident |
| | Family member |
| | Volunteer |
| | Employee |
| | Contractor |
| | Other (describe) |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 17 of 23 | |
| **Approved:** | | **Revised:** | |

## D. Risk Evaluation Summary

For each of the factors reviewed above, determine the risk rating. Refer to **Appendix C** as a guideline for assessment.

| **Risk Factor** | **Risk Rating** | | |
|---|---|---|---|
| | **Low** | **Medium** | **High** |
| 1) Containment | | | |
| 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 C** 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. | |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 18 of 23 | |
| **Approved:** | | **Revised:** | |

| Consideration | Description | Factor applies |
|---|---|---|
| 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 | Three Links 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 Three Links | Where Three Links 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 are 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.

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 19 of 23 | |
| **Approved:** | | **Revised:** | |

| **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 Three Links to control or reduce harm | |
| Steps individuals can take to protect themselves | |
| Future steps planned by Three Links to prevent further privacy breaches | |
| Three Links contact information for further assistance | |

**4) Others to contact**

| **Authority or organization** | **Reason for Contact** | **Applicable** |
|---|---|---|
| Law Enforcement | If theft or crime is suspected | |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 20 of 23 | |
| **Approved:** | | **Revised:** | |

| Authority or organization | Reason for Contact | Applicable |
|---|---|---|
| Insurers | Where required in accordance with an insurance policy | |
| Technology suppliers | If the breach was due to a technical falure and a recall or technical fix is required | |
| Others (list) | | |

**5) Confirm notifications completed**

| Key contact | Notified |
|---|---|
| Privacy Officer (Director of Human Resources) | |
| Your manager | |
| Chief Executive Officer | |
| Police | |
| Affected Individuals | |
| Legal Counsel | |
| Office of the Information and Privacy Commissioner of BC | |
| Others (list) | |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 21 of 23 | |
| **Approved:** | | **Revised:** | |

**Appendix C**

**PRIVACY RISK RATING OVERVIEW**

| **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, neighbours or co-workers<br>☑ Theft by stranger |
| **Cause of breach** | ☑ Technical error that has been resolved | ☑ Accidental loss or disclosure | ☑ Intentional breach<br>☑ Cause unknown<br>☑ Technical error – not resolved |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 22 of 23 | |
| **Approved:** | | **Revised:** | |

| **Risk Rating Overview** | | | |
|---|---|---|---|
| **Factor** | **Risk rating** | | |
| | **Low** | **Medium** | **High** |
| **Scope** | ☑ Very few individuals affected | ☑ Identified and limited group of affected individuals | ☑ Large group of entire scope of group not identified (over 50) |
| **Containment efforts** | ☑ Data was adequately encrypted<br>☑ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping<br>☑ 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<br>☑ 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<br>☑ Data, files or device have not been recovered<br>☑ 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<br>☑ Hurt, humiliation, damage to reputation or relationships | ☑ Security risk (eg. physical safety)<br>☑ Identity theft or fraud risk<br>☑ Hurt, humiliation, damage to reputation may |

| | | | |
|---|---|---|---|
| **Category:** | Administration Manual | **Number: AE0530** | |
| **Subject:** | Privacy Breach Management | **Page:** 23 of 23 | |
| **Approved:** | | **Revised:** | |

| **Risk Rating Overview** | | | |
|---|---|---|---|
| **Factor** | **Risk rating** | | |
| | **Low** | **Medium** | **High** |
| | | ☑ Social/ relational harm<br>☑ Loss of trust in Three Links<br>☑ Loss of Three Links assets<br>☑ Loss of Three Links contracts or business<br>☑ Financial exposure to Three Links including class action lawsuits | also be a high risk, depending on the circumstances<br>☑ Risk to public health or safety |