Privacy Breach Management Toolkit

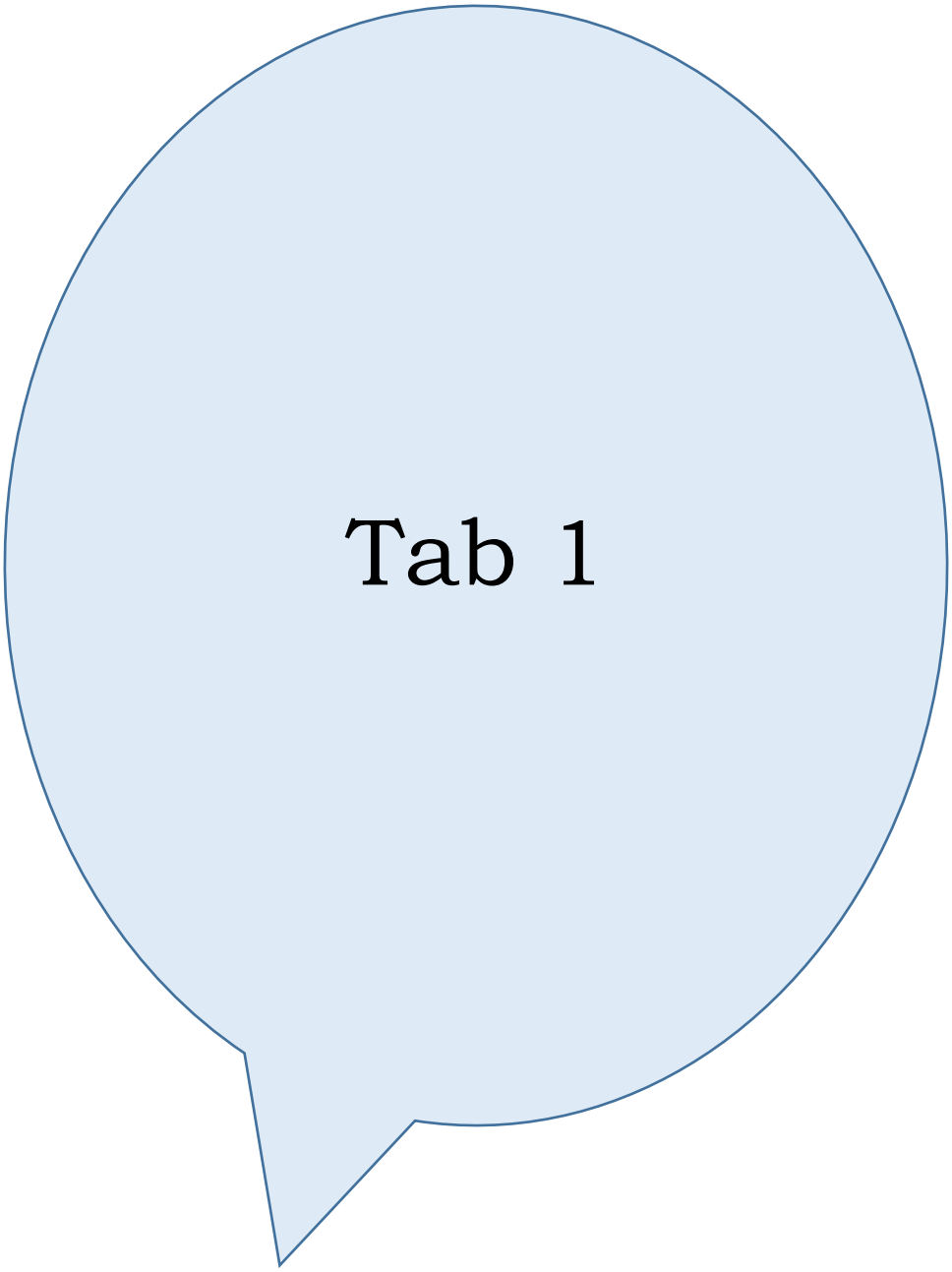
FOIPOP, MGA & PHIA

Office of the Information and Privacy Commissioner for Nova Scotia
oipcns@novascotia.ca 902-424-4684 https://oipc.novascotia.ca

Notice to Users

This document is intended to provide general information only. It is important to read the full legislation not just the sections summarized to understand the full extent of the provision. This document is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP, MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body, municipality or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each public body, municipality and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca

Contents


Tab 1

Freedom of Information and Protection of Privacy Act - Privacy Rules At a Glance

Privacy Rules		
24	Collection	• Public bodies shall not collect personal information unless: o The collection is expressly authorized by an enactment o The information is collected for the purpose of law enforcement o The information relates directly to and is necessary for an operating program or activity of the public body
24(2)	Accuracy	• If personal information will be used to make a decision that directly affects the individual the public body must ensure the information is accurate and complete
24(3)	Security	• The public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal
24(4)	Retention	• Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year
25	Correction	• Applicant may request a correction • Where no correction is made, the public body must annotate
26	Use	• A public body may use personal information only: o for the purpose for which that information was obtained or compiled or o for a use compatible with that purpose o if the individual has consented to the use o for a purpose for which the information may be disclosed to the public body under s. 27- 30
27	Disclosure (c) (b) (a) (d) (e) (f)	• A public body may disclose personal information only: **Compatible use & consent** o For the purpose the information was obtained or compiled or a use compatible with that purpose o If the individual has consented in writing to the disclosure **Note:** "compatible" is defined in s. 28 to mean a use of the personal information that has a reasonable and direct connection with the purpose for which it was originally collected <u>and</u> that is necessary for performing the statutory duties of, or for operating a legally authorized program of the public body. **Law, subpoena, court orders** o As provided pursuant to an enactment o For the purpose of complying with an enactment or with a treaty or agreement made pursuant to an enactment o To comply with a subpoena, warrant, summons or order issued by a court or person with jurisdiction to compel production of information **Public bodies** o To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee

Privacy Rules Cont'd		
27	Disclosure	**Public bodies cont'd**
	(g)	○ To a public body to meet the necessary requirements of government operations
	(h)	○ For the purpose of collecting a debt or fine owing to the Province or public body of to make a payment owed by the Province or public body
		Law-enforcement
	(m)	○ To a public body or a law-enforcement agency in Canada to assist in an investigation undertaken with a view to a law-enforcement proceeding or from which a law-enforcement proceeding is likely to result
	(n)	○ If the information is disclosed by a law-enforcement agency to another law-enforcement agency in Canada or in a foreign country under a written agreement, treaty or legislative authority
		Auditor, bargaining agent, public archives & research
	(i)	○ To the Auditor General for audit purposes
	(j)	○ To a member of the House of Assembly who has been requested by the individual, whom the information is about , to assist in resolving a problem
	(k)	○ To a representative or bargaining agent who has been authorized in writing by the employee whom the information is about to make an inquiry
	(l)	○ To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes
	(q)	○ For the purpose of research or to archives as set out in s. 29 & 30
		Safety
	(o)	○ If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
		Next of kin
	(p)	○ So next of kin or a friend of an injured, ill or deceased individual may be contacted

Notice

This table is intended as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Freedom of Information and Protection of Privacy Act* at: http://nslegislature.ca/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf

***Municipal Government Act* Privacy Rules – At a Glance**

Privacy Rules		
483	Collection	• Municipalities shall not collect personal information unless: o The collection is expressly authorized by an enactment o The information is collected for the purpose of law enforcement o The information relates directly to and is necessary for an operating program or activity of the municipality
483(2)	Accuracy	• If personal information will be used to make a decision that directly affects the individual the municipality must ensure the information is accurate and complete
483(3)	Security	• The municipality must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal
483(4)	Retention	• Where a municipality uses an individual's personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year
484	Correction	• Applicant may request a correction • Where no correction is made, the municipality must annotate
485(1)	Use	• A municipality may use personal information only: o for the purpose for which that information was obtained or compiled or o for a use compatible with that purpose o if the individual has consented to the use o for a purpose for which the information may be disclosed to the municipality under s. 485(2)
485(2)	Disclosure (c) (b) (a) (d) (e) (f)	• A municipality may disclose personal information only: **Compatible use & consent** o For the purpose the information was obtained or compiled or a use compatible with that purpose o If the individual has consented in writing to the disclosure **Law, subpoena, court orders** o As provided pursuant to an enactment o For the purpose of complying with an enactment or with a treaty or agreement made pursuant to an enactment o To comply with a subpoena, warrant, summons or order issued by a court or person with jurisdiction to compel production of information **Municipalities** o To an officer or employee of a municipality if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee

Privacy Rules Cont'd		
485(2)	Disclosure (g) (h) (l) (m) (i) (j) (k) 485(5) (na) 485(4) (p) (n)	**Municipalities cont'd** ○ To a municipality to meet the necessary requirements of municipal operation ○ For the purpose of collecting a debt or fine owing to the municipality or to make a payment owed by the municipality **Law enforcement** ○ To a municipality or a law-enforcement agency in Canada to assist in an investigation undertaken with a view to a law-enforcement proceeding or from which a law enforcement proceeding is likely to result ○ If the information is disclosed by a law-enforcement agency to another law enforcement agency in Canada or in a foreign country under a written agreement, treaty or legislative authority **Auditor, bargaining agent, public archives & research** ○ To the auditor for audit purposes ○ To a representative or bargaining agent who has been authorized in writing by the employee whom the information is about to make an inquiry ○ To the Public Archives of Nova Scotia, or the archives of a municipality for archival purposes ○ Archives of a municipality may disclose personal information for archival or historical purposes in limited circumstances ○ For the purpose of research or to archives as set out in s. 485(4) and (5) ○ For a research or statistical purpose in limited circumstances ○ For research or archival purposes **Safety** ○ If the responsible officer determines that compelling circumstances exist that affect anyone's health or safety **Next of kin** ○ So next of kin or a friend of an injured, ill or deceased individual may be contacted

Notice

This table is intended only as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Municipal Government Act* at:
http://nslegislature.ca/legc/statutes/municipal%20government.pdf

Personal Health Information Act - Privacy Rules At a Glance

A. Collection
- General Rule
- Best Practices
- Collection by non-custodian
- Indirect Collection

B. Use
- General Rule
- Best Practices
- Use by non-custodian
- Use by Agent
- Uses authorized or permitted under PHIA

C. **Disclosure**
- General Rule
- Best Practices
- Disclosures without consent – effect of authority
- Disclosures without consent – documentation required
- Disclosures by non-custodians
- Disclosures authorized or permitted under PHIA
  - Disclosures by recipient
  - Disclosures by purpose
  - Disclosures outside NS
  - Disclosures of deceased's phi

D. Health Card Number Rules

E. Consent Rules

F. Agents

G. Retention, Destruction, Security, Breach Reporting

Notice

This table is intended as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Personal Health Information Act* at https://nslegislature.ca/sites/default/files/legc/statutes/personal%20health%20information.pdf

A. Collection	
11	**General Rule** Health custodians shall not collect personal health information ("phi") unless • The custodians has the individual's consent and the collection is reasonably necessary for a lawful purpose or • The collection is permitted or required by this Act
24 25(1)	**Best Practice Requirements:** 1. **Collect non- phi first:** A custodian shall not collect phi if other information will serve the purpose of collection 2. **Minimum necessary:** Collection of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is collected.
26(1) 26(2)	**Application of s. 24 and 25 rules:** • These rules apply where the custodian is authorized to collect phi with knowledgeable implied consent, without consent and without consent unless the individual objects • These rules do not apply to phi that a custodian is required by law to collect
45(1) 38(5)	**Collection by non- custodian** • A non-custodian is authorized to collect the phi that a custodian may disclose to it but does not become a custodian merely by virtue of the collection • A prescribed entity that is not a custodian is authorized to collect the phi that the custodian may disclose to the prescribed entity under clause 38(1)(j)
31	**Indirect collection** A custodian shall collect directly from the individual about whom the information is being collected except: a. **Consent:** If the individual authorizes indirect collection b. **Substitute Decision Maker:** The collection is from the substitute decision-maker ("SDM) if the SDM has authority to act c. **Inaccurate or not timely**: The information is reasonably necessary for providing health care and it is not reasonably possible to collect directly from the individual phi that can be reasonably relied on as accurate or phi in a timely manner d. **Safety:** direct collection would prejudice the safety of any individual e. **Family history:** collection is to assemble family history in the context of providing health care f. **Eligibility for program**: collection is in the course of processing an application for a benefit or program **g. Breach of agreement or proceedings:** The custodian is a public body under FOIPOP and is collecting the information for a purpose related to investigating a breach of an agreement, to conduct a proceeding or in relation to a statutory function of the custodian h. **Research:** Custodian is collecting for a research project approved by a research ethics board **i. Prescribed entity:** Custodian is a prescribed entity **j. Treaty or agreement:** Custodian collects the info from a person who is permitted or required by law, treaty or agreement made under this or another Act to disclose it to the custodian **k. Permitted or required by law:** Custodian collects as permitted or required by law or treaty **l. Minister of Health:** Collection by minister for the purpose of planning or managing the health system **m. Quality or standards of care:** Collection is for the purpose of ensuring quality or standards of care within a quality review program **n. Payments:** collection is reasonably necessary for the administration of payments in connect with the provision for health care **o. Minister of Health:** Collection is from another custodian for the purpose of creating or maintaining an electronic health record

B. Use	
11	**General Rule** Health custodians shall not use personal health information unless • The custodians has the individual's consent and the use is reasonably necessary for a lawful purpose or • The use is permitted or required by this Act
24 25(1) 25(2)(a) 26(1) 26(2)	**Best Practice Requirements:** 1. **Use non-phi first:** A custodian shall not use phi if other info will serve the purpose of the use 2. **Minimum necessary:** Use of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is used. 3. **Agents need to know:** Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act **Application of s. 24 and 25 rules:** • These rules apply where the custodian is authorized to use phi with knowledgeable implied consent, without consent and without consent unless the individual objects • These rules do not apply to phi that a custodian is required by law to use
    45(2)(a) 45(2)(b)	**Use by non-custodian** A non-custodian (to whom a custodian has disclosed phi) shall not use phi for any purpose other than • For the purpose the custodian was authorized to disclose the information under PHIA or • For the purpose of carrying out a legal duty A non-custodian shall not use more information than is reasonably necessary to meet the purpose of the use, unless the use is required by law.
25(2)(a) 29(1) 29(2) 33(c) 35(2)	**Use by agent** • **Need to know:** Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act • **Authority:** Where a custodian is authorized to use phi for a purpose, the custodian may provide the information to an agent who may use it for that purpose on behalf of the custodian. • **Use not disclosure or collection:** For the purpose of PHIA, the providing of phi between a custodian and an agent of the custodian is a use by the custodian and not a disclosure by the custodian or a collection by the agent • **Education:** A custodian may use phi for educating agents to provide health care • **Non-consensual use:** Where custodian is authorized to use phi without consent, the custodian may provide the information to an agent of the custodian who may use if for that purpose on behalf of the custodian
33	**Uses permitted or required under PHIA** a) **Use for original purpose**: A custodian may use phi for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose b) For purposes which this Act or another Act permit or requires a personal to disclose it to the custodian or c) For the purpose of educating agents to provide health care.

Uses Authorized or Permitted Under PHIA				
Type of information or use	**PHIA provision**	**Express Consent**	**Implied Consent**	**No consent = statutory authority**
Circle of care – within health care facilities	12, 25(2)(a)		•	•
Consent – may use phi to seek consent – limited to name & contact info	35(1)(e)			•
De-identification	35(1)(d)			•
Educating agents to provide health care	33(c)			•
Electronic Health Record – to create or maintain if the custodian is the Minister	35(1)(ha)			•
Fraud prevention – detect & monitor unauthorized receipt of services or benefits	35(1)(b)			•
Fundraising activities	34(a)	•		
Law – for a purpose permitted under PHIA or another Act	33(b)			•
Law – permitted or required by law or treaty made under PHIA or another Act	35(1)(i)			•
Legal proceeding	35(1)(f)			•
Market research, commercial purpose	34(b)	•		
Original purpose collected and functions reasonably necessary to carry out that purpose	33(a)			•
Payment processing – obtaining, verifying reimbursing claims for payment	35(1)(g)			•
Planning and delivery or programs	35(1)(a)			•
Quality review program	35(1)(c)			•
Research conducted by the custodian • Must use minimum amount of info necessary (s. 54) • Must comply with s. 55	35(1)(h)			•
Risk Management	35(1)(j)			•

C. Disclosure	
11	**General Rule** Health custodians shall not disclose personal health information unless • The custodians has the individual's consent and the disclosure is reasonably necessary for a lawful purpose or • The disclosure is permitted or required by this Act
	Best Practice Requirements
24	1. **Disclose non-phi first:** A custodian shall not disclose phi if other information will serve the purpose of disclosure
25(1)	2. **Minimum necessary:** Disclosure of phi must be limited to the minimum amount of phi necessary to achieve the purpose for which it is disclosed.
25(2)(b)	3. **Circle of care – facilities:** Custodians shall limit disclosure of phi to those regulated health professionals who have the right to treat individuals in the custodian's health care facility, to only that information that the health professionals require to carry out their duties and responsibilities
36	4. **Circle of care – generally:** Custodians may disclose phi to a custodian involved in the individual's health care if the disclosure is reasonably necessary for the provision of health care to the individual
	Application of s. 24 and 25 rules:
26(1)	• These rules apply where the custodian is authorized to disclose phi with knowledgeable implied consent, without consent and without consent unless the individual objects
26(2)	• These rules do not apply to phi that a custodian is required by law to disclose
	Disclosures without consent – effect of authority
	A provision in this Act that permits a custodian to disclose phi without consent
10(2)	• does not require the custodian to disclose it unless required to do so by law, • does not relieve the custodian from a legal requirement to disclose the information and • does not prevent the custodian from obtaining the individual's consent for the disclosure or giving notice to the individual of the disclosure
41(1)	• A provision of PHIA that permits disclosure without consent does not prevent the custodian from obtaining the individual's consent to disclosure (except where disclosure is required by law)
	Disclosures without consent – documentation required

42(1)	• Disclosures without consent must be documented
	• Documentation must include:
	  ○ Description or copy of phi disclosed
	  ○ Name of person or organization to whom the phi was disclosed
	  ○ Date of disclosure
	  ○ Authority for disclosure

	Disclosure by non-custodian
45(2)	A non-custodian (to whom a custodian disclosed the phi) shall not disclose phi for any purpose other than • For the purpose the custodian was authorized to disclose the information under PHIA or • For the purpose of carrying out a legal duty
45(3)	A non-custodian shall not disclose more information than is reasonably necessary to meet the purpose of the disclosure, unless the disclosure is required by law.

Disclosures authorized or permitted under PHIA				
Type of information or disclosure	**PHIA provision**	**Express Consent**	**Implied Consent**	**No consent = statutory authority**
Disclosure by Recipient				
CIHI – Canadian Institute for Health Information • For planning and management	38(1)(i)			•
Circle of care • Generally • Within custodian's facility	12, 36 12, 25(2)(b)		• •	• •
Family/Close personal relationship • Information related to deceased family member • General information about presence & general condition of individual on day information not contrary to express request	40(1) & (2) 37		 •	• •
Correctional Facility • to allow the provision of health care	38(1)(e)			•
Custodian • Reasonably necessary for the provision of care • Not for health care • To prevent fraud, an offence or assist in investigation under enactment • Within a quality review program • To determine or verify eligibility for insured services	36 43(b) 38(1)(a) 38(1)(f) 38(1)(m)	 •	•	 • • •
Legal Advisor • An agent who receives phi for the purpose of a proceeding or contemplated proceeding may disclose the information the agent's or former agent's professional advisor for the purpose of providing advice or representation	38(7)			•
Legal Guardian • acting on behalf of the individual	38(1)(b)(ii)			•
Litigation Guardian • for purpose of appointment • to commence or defend legal action	38(1)(o) 38(1)(p)			• •
Media	43(e)	•		
Minister • For planning and management of health system • For purpose of creating or maintaining an EHR	38(1)(g) 38(1)(u)			• •

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by Recipient continued				
Non-custodian • Generally unless authorized by law • To avert or minimize an imminent risk to any person • For risk management within the custodian's organization • To facilitate assessment, care or treatment and with authorization of Minister • Administration of payments for health care • Risk management or patient safety within the custodian's organization	 43(a) 38(1)(d) 38(1)(t) 39 38(1)(r) 38(1)(t)	 •		 • • • • •
Prescribed entities • For planning and management subject to conditions in 38(2)	 38(1)(j)			 •
Prescription Monitoring Board • For monitoring prescriptions pursuant to the Prescription Monitoring Act	 38(1)(h)			 •
Provincial or territorial government • From the Province to another for planning and management	 38(1)(k)			 •
Representative, litigation guardian, administrator • To persons acting on behalf of the individual • Proposed litigation guardian or legal representative for the purpose of having them appointed as such • Litigation guardian or legal representative authorized to commence or defend a proceeding	 38(1)(b) 38(1)(o) 38(1)(p)			 • • •
Regulated health profession body • For the purpose of carrying out its duties under provincial or federal law	 38(1)(c)			 •
Researcher – unless s. 57 applies	38(1)(f)	•		
Researcher – with plan, REB approval and agreement	57			•
Substitute Decision Maker • Person legally entitled to make health-care decisions on behalf of the individual • Legal Guardian • Estate Administrator	 38(1)(b)(i) 38(1)(b)(ii) 38(1)(b)(iii)			 •
Within health care facility/custodian organization • Circle of care disclosures • Risk management or patient safety	 25(3) 38(1)(t)		•	 • •

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by purpose				
Administer estate • To the administrator of an estate if the disclosure is for the purpose of the estate	38(1)(b)(iii)			•
Eligibility for insured services • To another custodian to verify or determine eligibility for insured services • Administration of payments in connection with health care	38(1)(m) 38(1)(r)			•
Electronic Health Record • To Minister for the purpose of creating or maintaining an HER	38(1)(u)			•
Family concerns • Information related to deceased family member • General information about presence & general condition of individual on day information not contrary to express request	40(1) & (2) 37		•	• •
Fraud or offence detection & prevention • To another custodian to prevent or assist an investigation of fraud in the use of health services or prevent commission of offence	38(1)(a)			•
Fund raising	43(c)	•		
Insured services • To another custodian to verify or determine eligibility for insured services	38(1)(m)			•
Law, treaty or arrangement • Disclosures required or permitted by law, treaty or arrangement made pursuant to PHIA or another Act	38(1)(l)			•
Legal proceedings • For purpose of legal proceeding in which the custodian or agent is a party or witness • To appoint litigation guardian or legal representative • To commence or defend litigation • To comply with summons, order or procedural rule	38(1)(s) 38(1)(o) 38(1)(p) 38(1)(q)			 • • •
Marketing and service for a commercial purpose	43(d)	•		
Market research	43(d)	•		
Offence prevention • To another custodian if the disclosure will prevent the commission of an offence under and enactment	38(1)(a)			•
Payment for healthcare	38(1)(r)			•
Prescription monitoring – to PM Board only	38(1)(h)			•

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Disclosure by purpose continued				
Planning & management of the health system • CIHI in accordance with agreement • Minister • Prescribed entities • Provinces & territories • Planning & management does not = research	 38(1)(i) 38(1)(g) 38(1)(j) 38(1)(k) 53			 • • • •
Quality review program	38(1)(f)			•
Regulation of professions (to colleges) • Information required for the purpose of carrying out its duties under an Act	38(1)(c)			•
Research generally (unless s.57 applies)	43(f)	•		
Risk management within the custodian's organization	38(1)(t)			•
Safety – to avert or minimize imminent danger	38(1)(d)			•
Treatment related • To correctional facility in which the individual is being lawfully detained to allow the provision of health care • To custodian where reasonably necessary for provision of care (circle of care) • To non-custodian for the purpose of facilitating assessment, care or treatment with authorization of Minister • To person acting on behalf of the individual who is legally entitled to make health care decisions • To family member or close relationship information about presence and condition • Outside NS where reasonably necessary for the provision of health care and no express instruction to the contrary	 38(1)(e) 36 39 38(1)(b) 37 44(1)(e)	 •	 •	 • • • • •
Disclosure outside NS				
Outside NS – generally with consent	44(1)(a)		•	
Outside NS – permitted by PHIA	44(1)(b)			•
To a regulated health professional – prescription monitoring	44(1)(c)			•
Planning and management of health care	44(1)(d)			•
Info relates to health care provided in NS to an individual who resides outside NS	44(1)(d)			•
To the government of a province or Canada	44(1)(d)			•
Reasonably necessary for provision of health care	44(1)(e) 44(2)	•		•

Type of information or disclosure	PHIA provision	Express Consent	Implied Consent	No consent = statutory authority
Deceased (PHI relating to deceased persons)				
• For the purpose of identifying the individual	40(1)(a)			•
• To inform any person that the individual is deceased	40(1)(b)			•
• To listed relatives if the information is needed to make health care decisions	40(1)(c)			•
• For carrying out the deceased person's wishes for the purpose of tissue donation	40(1)(d)	•		
• Info relating to circumstances of death to family members or close personal relationship – so long as not contrary to a prior express request of the individual	40(2)		•	•
• To estate administrator for purpose of the estate	38(1)(b)(iii)			•

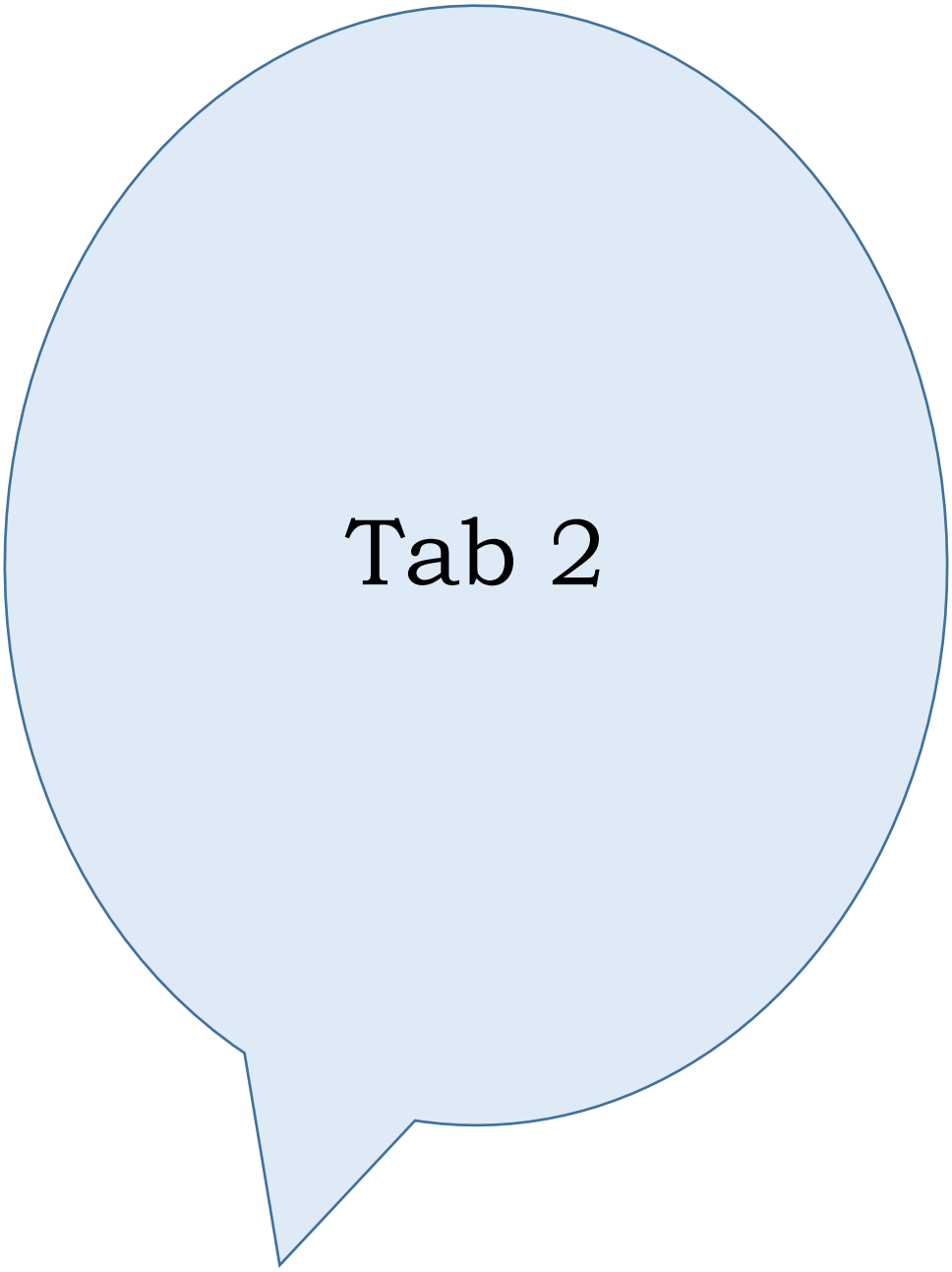
D. Health Card Number Rules	
27	A person who is not a custodian or authorized by the regulations (reg. 6) shall not collect or use an individual's health card number
Reg. 6	For the purposes of clause 27 the following non-custodians are authorized to collect and use an individual's health card number for the purposes specified: • WCB – assess worker's entitlement to benefits • MCS – facilitate health care for children, indicate eligibility for pharmacare program, determine benefits • MSNS and MR – Vital Statistics division for registering births and deaths • Office of Public Trustee – facilitate health care decisions for clients • Mi'kmaw First Nations band to create and maintain NS FN Client Linkage Registry
Reg. 7	Non custodian is authorized to collect and use an individual's health cared number for the purposes of facilitating the provision of insured services
46	Notwithstanding any enactment except the Juries Act and the Elections Act the Minister has the sole authority for deciding who may have access to the information in the health cared number database, the Common Client Registry or any successor client information system related to the health card number.

E. Consent Rules Summary	
11	**General Rule** A custodian shall not collect, use or disclose ("cud") phi unless • The custodian has the individual's consent under this Act and the cud is reasonably necessary for a lawful purpose; or • The cud is permitted or required by this Act
10(1)	**"With consent" rule doesn't affect "without consent" rules** • A provision of this Act that applies to cud of phi with consent, does not affect the cud that this Act permits or requires without consent
12	**Knowledgeable implied consent - acceptable** Unless this Act requires express consent or makes exception to the requirement for consent, knowledgeable implied consent may be accepted as consent for cud of phi
32, 34 43	**Express consent requirements** • Express consent is required for <u>collection and use</u> of phi for market research, marketing any service for a commercial purpose and fundraising • Express consent is required for <u>disclosure</u> of phi o By custodian to non-custodian unless required or authorized by law o By a custodian to another custodian if it is not for the purpose of providing health care unless required or authorized by law o For fund-raising activities o For market research or marketing any service for a commercial purpose o To media o To a personal or organization for the purpose of research unless provided for in s. 57
13	**Requirements for consent** For both knowledgeable implied consent and express consent, the consent must: • Be a consent of the individual • Be knowledgeable • Relate to the specific information at issue and • Be voluntary
14	"**Knowledgeable"** Consent to cud of phi is knowledgeable if it is reasonable in the circumstances to believe that the individual knows: • The purpose of the cud as the case may be and • That the individual may give or withhold consent

Consent Rules continued	
15	"**Reasonable"** It is reasonable to believe that an individual knows the purpose of cud of phi if the custodian: • Makes readily available a notice describing the purpose in a manner that the purpose is likely to come to the individual's attention or • Explains the purpose to the individual • Unless language or reading barrier
17	**Revocation** An individual may limit or revoke consent to collection, use or disclosure of phi. • Revocation is not retroactive • Custodian must take reasonable steps to comply • Custodian shall inform the individual of the consequences of limiting or revoking consent • Custodian shall notify custodian to whom phi is disclosed of limitations • Revocation does not apply to phi that a custodian is required by law to cud
18	**Age & capacity** Any capable individual, regardless of age may consent or withdraw consent for the purpose of PHIA
20	**Capacity includes** Where an individual is deemed to have the capacity to consent to cud of phi, this capacity includes disclosure to a parent, guardian or substitute decision-maker where applicable.
3(b)	**Definition of "capacity"** Means the ability to understand information that is relevant to the making of a decision related to the cud of phi and the ability to appreciate the reasonably foreseeable consequences of a decision or lack of decision
	Substitute decision maker Consent to cud may be given by a substitute decision maker (SDM) if the individual lacks the capacity to make the decision

F. Agents	
3(a)	**Agent**, in relation to a custodian means a person who, with authorization of the custodian, acts for or on behalf of the custodian in respect of phi. Includes an employee, volunteer, insurer, lawyer or liability protection provider.
6(2)	**Regulated health professionals:** Except as prescribed, a regulated health professional is not a custodian in respect of phi that the person collects, uses or discloses while performing the person's powers or duties when an agent of a custodian.
28	**General rule:** A custodian may permit the custodian's agent to cud, retain, destroy or dispose of phi on the custodian's behalf only if: • The custodian is permitted or required to cud, retain, destroy, or dispose of the phi • The cud, retention, destruction or disposition of the information is in the course of the agent's duties and not contrary to the limits imposed by the custodian, this Act or another law and • The prescribed requirements, if any, are met (none currently)
25(2)(a) 29(1) 29(2) 33(c) 35(2)	**Use** • **Need to know:** Use of phi by agents of custodian shall be limited to those of its agents who need to know the information to carry out the purposes for which it was collected or a purpose authorized under this Act • **Authority:** Where a custodian is authorized to use phi for a purpose, the custodian may provide the information to an agent who may use it for that purpose on behalf of the custodian. • **Use not disclosure or collection:** For the purpose of PHIA, the providing of phi between a custodian and an agent of the custodian is a use by the custodian and not a disclosure by the custodian or a collection by the agent • **Education:** A custodian may use phi for educating agents to provide health care • **Non-consensual use:** Where custodian is authorized to use phi without consent, the custodian may provide the information to an agent of the custodian who may use if for that purpose on behalf of the custodian
38(7)	**Disclosure** • An agent who receives phi for the purpose of a proceeding or contemplated proceeding may disclose the information the agent's or former agent's professional advisor for the purpose of providing advice or representation

G. Retention, Destruction, Security, Breach Reporting	
50(1) 51 49(2)	**Retention Rule** • Custodian must have a written retention schedule for PHI • Custodian must follow retention schedule • At expiry of relevant retention period PHI must be securely destroyed, erased or de-identified.
49(2)	**Destruction Rule** • Must securely destroy (erase or de-identify) phi at expiry of relevant retention period
61 62(c)	**Security Rule** • Custodian shall protect confidentiality of phi • Shall protect against theft, loss, unauthorized access to or use, disclosure, copying or modification of information
69 70	**Breach Reporting** • Must notify affected individual at first reasonable opportunity if the custodian believes information is stolen, lost, subject to unauthorized access, use, disclosure, copying and, as a result, there is a potential for harm or embarrassment to the individual • Where the custodian believes on a reasonable basis that there is no potential for harm or embarrassment, notification of the affected individual is not required but the custodian shall notify the Review Officer as soon as possible


Tab 2

Key Steps to Responding to Privacy Breaches[1]

What is a privacy breach?

A privacy breach occurs whenever there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is unauthorized if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), the *Municipal Government Act Part XX* (*MGA*) or the *Personal Health Information Act* (*PHIA*).

What are the four key steps?

Step 1: Contain the Breach
Step 2: Evaluate the Risks
Step 3: Notification
Step 4: Prevention

The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. The fourth step is undertaken once the causes of the breach are known, in an effort to find longer term solutions to the identified problem.

Purpose of the Key Steps Document

Privacy breaches take many different forms, from misdirected faxes containing tax data, to the loss of hard drives containing personal information, to medical files blowing out the back of a garbage truck. Public bodies, municipalities and health custodians in Nova Scotia should be prepared to manage their responses to privacy breaches. The four key steps to responding to privacy breaches are steps that have been adopted across most Canadian jurisdictions in both the public and private sector. They represent best privacy practices for mitigating the harm arising from a privacy breach.

Use this document in combination with the Privacy Breach Checklist (p. 12 of this document) also available on our website at https://oipc.novascotia.ca.

[1] This document is adapted from material prepared by the Office of the Information Commissioner of British Columbia entitled: *Privacy Breaches: Tools and Resources* available at https://www.oipc.bc.ca/tools-guidance/guidance-documents.

Step 1: Contain the Breach

Before continuing, you should ensure that you record all steps taken to investigate and manage the breach. The Privacy Breach Checklist tool can be used to complete all of the steps set out below and to record all relevant information. That tool is available at p. 12 of this document and at: https://oipc.novascotia.ca.

You should take immediate and common sense steps to limit the breach including:

- **Contain:** Immediately contain the breach by, for example, stopping the unauthorized practice, shutting down the system that was breached, revoking or changing computer access codes, sending a remote "kill" signal to a lost or stolen portable storage device, correcting weaknesses in physical security or searching the neighborhood or used item websites (such as Kijiji) for items stolen from a car or house.

- **Initial Investigation:** Designate an appropriate individual to lead the initial investigation. Begin this process the day the breach is discovered. This individual should have the authority within the public body or organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

- **Privacy Officer & Other Internal Notifications:** Immediately contact your Privacy Officer and the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this stage. It is helpful to prepare in advance a list of all of the individuals who should be contacted along with current contact information.

- **Breach Response Team:** Determine whether a breach response team must be assembled which could include representatives from appropriate business areas (labour relations, legal, communications, senior management). Representatives from privacy and security should always be included and generally the privacy team is responsible for coordinating the response to the incident.

- **Police:** Notify the police if the breach involves theft or other criminal activity.

- **Preserve Evidence:** Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause, or, that will allow you to take appropriate corrective action.

Step 2: Evaluate the Risks

To determine what other steps are immediately necessary, you must assess the risks. Consider the following factors:

Personal Information Involved

- As soon as possible get a complete list of all of the personal information at risk. Generally this means developing a list of the data elements lost, stolen or inappropriately accessed. For example, the data could include, name, address, date of birth, medical diagnosis and health card number (MSI). At this stage it is important that the investigator confirm the data at risk as quickly as possible. Be aware that if the breach is caused by an error or oversight by an employee, he or she may be reluctant to fully disclose the scope of the lost data.

- Next, evaluate the sensitivity of the personal information. Some personal information is more sensitive than others. Generally information including health information, government-issued pieces of information such as social insurance numbers, health care numbers and financial account numbers such as credit card numbers, is considered sensitive.

- Also consider the context of the information when evaluating sensitivity. For example, a list of customers on a newspaper carrier's route may not be sensitive. However, a list of customers who have requested service interruption while on vacation would be more sensitive.

- Finally, in your evaluation of sensitivity, consider the possible use of the information. Sometimes it is the combination of the data elements that make the information sensitive or capable of being used for fraudulent or otherwise harmful purposes.

- The more sensitive the information, the higher the risk.

Cause and Extent of the Breach

The cause and extent of the breach must also be considered in your analysis of the risks associated with the breach. Answer all of the following questions:

- 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?
- Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Is the information encrypted or otherwise not readily accessible?
- Has the personal information been recovered?
- What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

Individuals Affected by the Breach

Knowing who was affected by the breach will shape your strategies in managing the breach and may also determine who will help manage the breach (e.g. union employees affected likely means labour relations should be on the breach management team), it will also determine who you decide to notify – if business partners are affected, then you will likely want to notify them.

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

Foreseeable Harm from the Breach

- Who is in receipt of the information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.

- Is there any relationship between the unauthorized recipients and the data subject? A close relationship between a victim and the recipient may increase the likelihood of harm – an estranged spouse is more likely to misuse information than a neighbour.

- What harm to the individuals will result from the breach? Harm that may occur includes:
    - Security risk (e.g. physical safety);
    - Identity theft or fraud;
    - Loss of business or employment opportunities;
    - Hurt, humiliation, damage to reputation or relationships;
    - Basis for potential discriminatory action that may be taken against the individual;
    - Social/relational harm (damage to the individual's relationships).

- What harm could result to the public body or organization as a result of the breach? For example:
    - Loss of trust in the public body or organization
    - Loss of assets
    - Financial exposure including class action lawsuits
    - Loss of contracts/business

- What harm could result to the public as a result of the breach? For example:
    - Risk to public health
    - Risk to public safety

Once you have assessed all of the risks described above you will be able to determine whether or not notification is an appropriate mitigation strategy. Further, the risk assessment will help you to identify appropriate prevention strategies.

The table below summarizes the risk factors and suggests a **possible** risk rating. Each public body, health custodian or municipality must make its own assessment of the risks given the unique circumstances of the situation. 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 the 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 ex-partners, 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

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 public body ✓ Loss of public body assets ✓ Loss of public body contracts or business ✓ Financial exposure to public body 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

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit the public body, municipality, health custodian and the individuals affected by a breach. Prompt notification can help individuals mitigate the damage by taking steps to protect themselves. The challenge is to determine when notice should be required. Each incident needs to be considered on a case-by-case basis to determine whether the privacy breach notification is required. In addition, public bodies, municipalities and health custodians are encouraged to contact the Office of the Information and Privacy Commissioner for Nova Scotia for assistance in managing a breach.[2]

Review your risk assessment to determine whether notification is appropriate. If sensitive information is at risk, if the information is likely to be misused, if there is foreseeable harm, then you will likely want to notify. The list below provides further information to assist in decision making.

Note to health custodians: There are additional considerations set out specifically in *PHIA*. In particular, *PHIA* requires notification be given to either the affected individual or the Information and Privacy Commissioner in accordance with ss. 69 and 70 of *PHIA*.

Neither *FOIPOP* nor *Part XX* of the *MGA* requires notification. However, as noted above, notification in appropriate circumstances is best privacy practice and will help mitigate the losses suffered by individuals as a result of the breach. The steps taken in response to a breach have the potential to significantly reduce the harm caused by the breach, which will be relevant in any lawsuit for breach of privacy.

Notifying affected individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Legislation requires notification – s. 69 and s. 70 of *PHIA* for example;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud – usually because of the type of information lost, stolen, accessed or disclosed, such as a SIN, banking information, identification numbers;
- There is a risk of physical harm – if the loss puts an individual at risk of stalking or harassment;

[2] The Office of the Information and Privacy Commissioner for Nova Scotia has the responsibility for monitoring how privacy provisions are administered and the ability to provide advice and comments on the privacy provisions when requested by public bodies and custodians. Our contact information is included on the last page of this document.

- There is a risk of hurt, humiliation or damage to reputation – for example when the information lost includes medical or disciplinary records;
- There is a risk of loss of business or employment opportunities – if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities; and
- There is a risk of loss of confidence in the public body or organization and/or good citizen relations dictates that notification is appropriate.

When and How to Notify

Notification should occur as soon as possible following the breach – within days whenever possible. 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.

On very rare occasions, medical evidence may indicate that notification could reasonably be expected to result in immediate and grave harm to the individual's mental or physical health. In those circumstances, consider alternative approaches, such as having the physician give the notice in person or waiting until the immediate danger has passed.

Direct notification is preferred – by phone, by letter or in person. Indirect notification – via websites, posted notices or media reports – should generally only occur in rare circumstances such as where direct notification could cause further harm or contact information is lacking.

Using multiple methods of notification in certain cases may be the most effective approach.

What Should be Included in the Notification?

Notifications should include the following information:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Where there is a risk of identity theft as a result of the breach, typically the notice should offer free credit watch protection as part of the mitigation strategy;
- Further steps planned to prevent future privacy breaches;

- Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's license number);

- Contact information of an individual within the public body, municipality or health organization who can answer questions or provide further information;

- Information and Privacy Commissioner for Nova Scotia contact information and the fact that individuals have a right to complain to the Information and Privacy Commissioner under the *Privacy Review Officer Act* and *PHIA*. If the public body, municipality or health custodian has already contacted the Information and Privacy Commissioner, include this detail in the notification letter.

Other Sources of Information

As noted above, the breach notification letter should include a contact number within the public body, municipality or health custodian, in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to further inquiries.

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police – if theft or other crime is suspected;

- Insurers or others - if required by contractual obligations;

- Professional or other regulatory bodies - if professional or regulatory standards require notification of these bodies;

- Other internal or external parties not already notified – your investigation and risk analysis may have identified other parties impacted by the breach such as third party contractors, internal business units or unions;

- Office of the Information and Privacy Commissioner for Nova Scotia - the mandate of the Office of the Information and Privacy Commissioner includes a responsibility to monitor how the privacy provisions are administered and to provide advice and comments on the privacy provisions when requested by public bodies and health custodians.

The following factors are relevant in deciding whether or not to report a breach to the Office of the Information and Privacy Commissioner for Nova Scotia:

- For health custodians, s. 70 of *PHIA* sets out when the Office of the Information and Privacy Commissioner for Nova Scotia must be contacted. Health custodians may wish to contact the

Office of the Information and Privacy Commissioner even when notification is not required, based on some of the factors listed below:

- The sensitivity of the information – generally the more sensitive the information at risk, the more likely the Office of the Information and Privacy Commissioner for Nova Scotia will be notified;
- Whether the disclosed information could be used to commit identity theft;
- Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;
- The number of people affected by the breach;
- Whether the information was fully recovered without further disclosure;
- Your public body, municipality or health custodian wishes to seek advice or comment from the Information and Privacy Commissioner to aid in managing the privacy breach;
- Your public body, municipality or health custodian requires assistance in developing a procedure for responding to the privacy breach, including notification;
- Your public body, municipality or health custodian is concerned that notification may cause further harm; and/or
- To ensure steps taken comply with the public body's obligations under privacy legislation.

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 further breaches.

Typically, prevention strategies will address privacy controls in all of the following areas:

- Physical
- Technical
- Administrative
- Personnel

So, for example, if any physical security weaknesses contributed to the breach, changes made to prevent a recurrence should be undertaken. Systems controls should also be reviewed to ensure that all necessary technical safeguards are in place. This could mean encrypting all portable storage devices or improving firewall protections on a database.

Administrative controls would include ensuring that polices are reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Staff of public bodies, municipalities and health custodians should be trained to know the organization's privacy obligations under *FOIPOP*, *MGA Part XX* and/or *PHIA*.

In the longer term, public bodies, health custodians and municipalities should review and refresh their privacy management framework to ensure that they continue to comply with their privacy obligations. For more information on privacy management frameworks visit the Office of the Information and Privacy Commissioner for Nova Scotia website at: https://oipc.novascotia.ca.

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 for Nova Scotia.[3] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: https://oipc.novascotia.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

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

_____

_____

_____

_____

[3] The Office of the Information and Privacy Commissioner for Nova Scotia's mandate includes an obligation to monitor how privacy provisions are administered and to provide advice and comments on privacy provisions on the request of health custodians and public bodies.

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 16.

(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 is 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.
    - ❑ 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:

_____

_____

_____

_____

(2) 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) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ 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 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 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)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

_____

(7) 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
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

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

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 from the breach			
7) 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

(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. 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.	

(2) 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	

(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 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 for Nova Scotia	
Public body, municipality or health custodian contact information – for further assistance	

(4) 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:	
Technology suppliers	
Others (list):	

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,[4] and assess if any further adjustments are necessary as part of your prevention strategy.

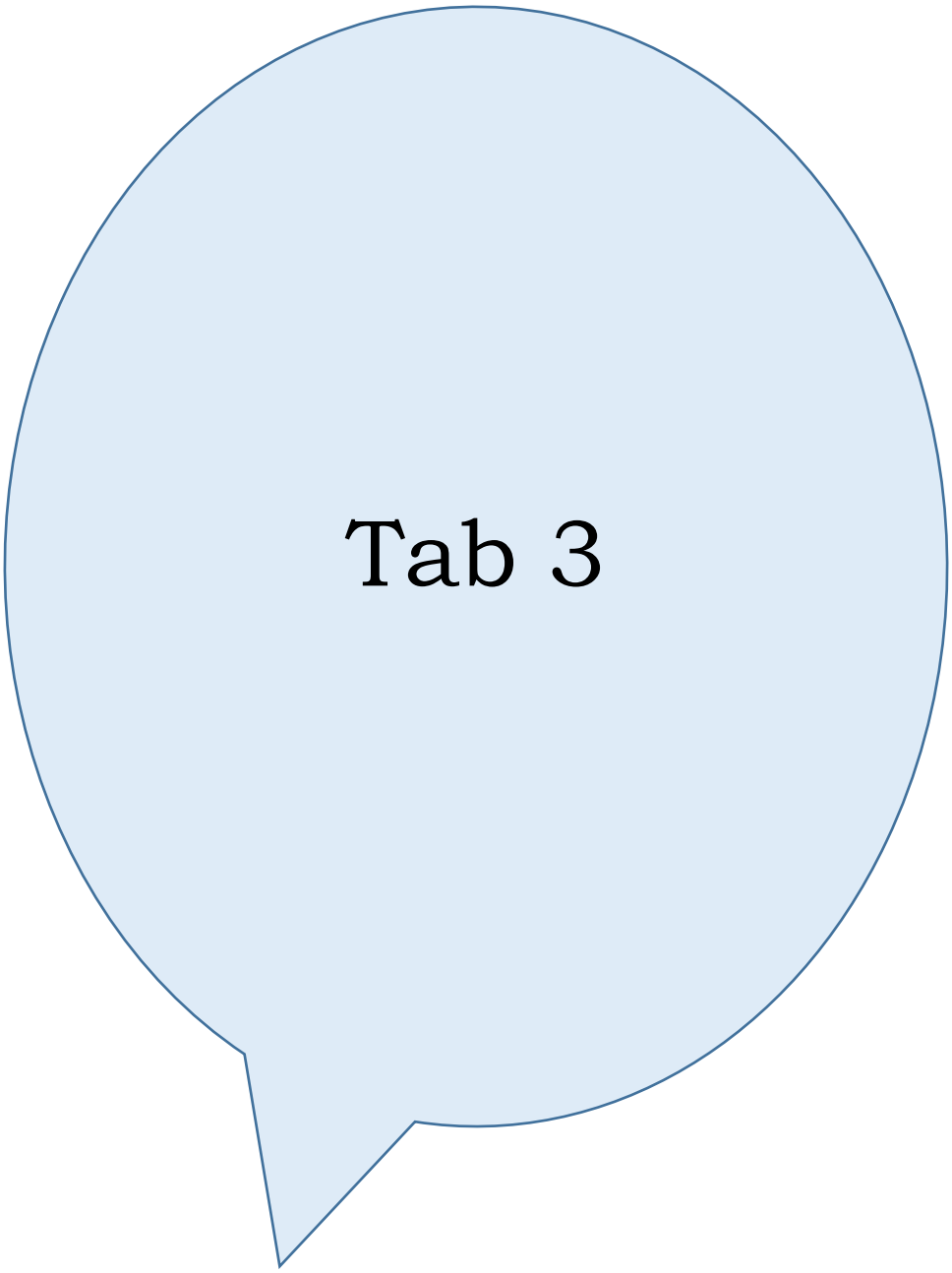
Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

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?

[4] For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: https://oipc.novascotia.ca.

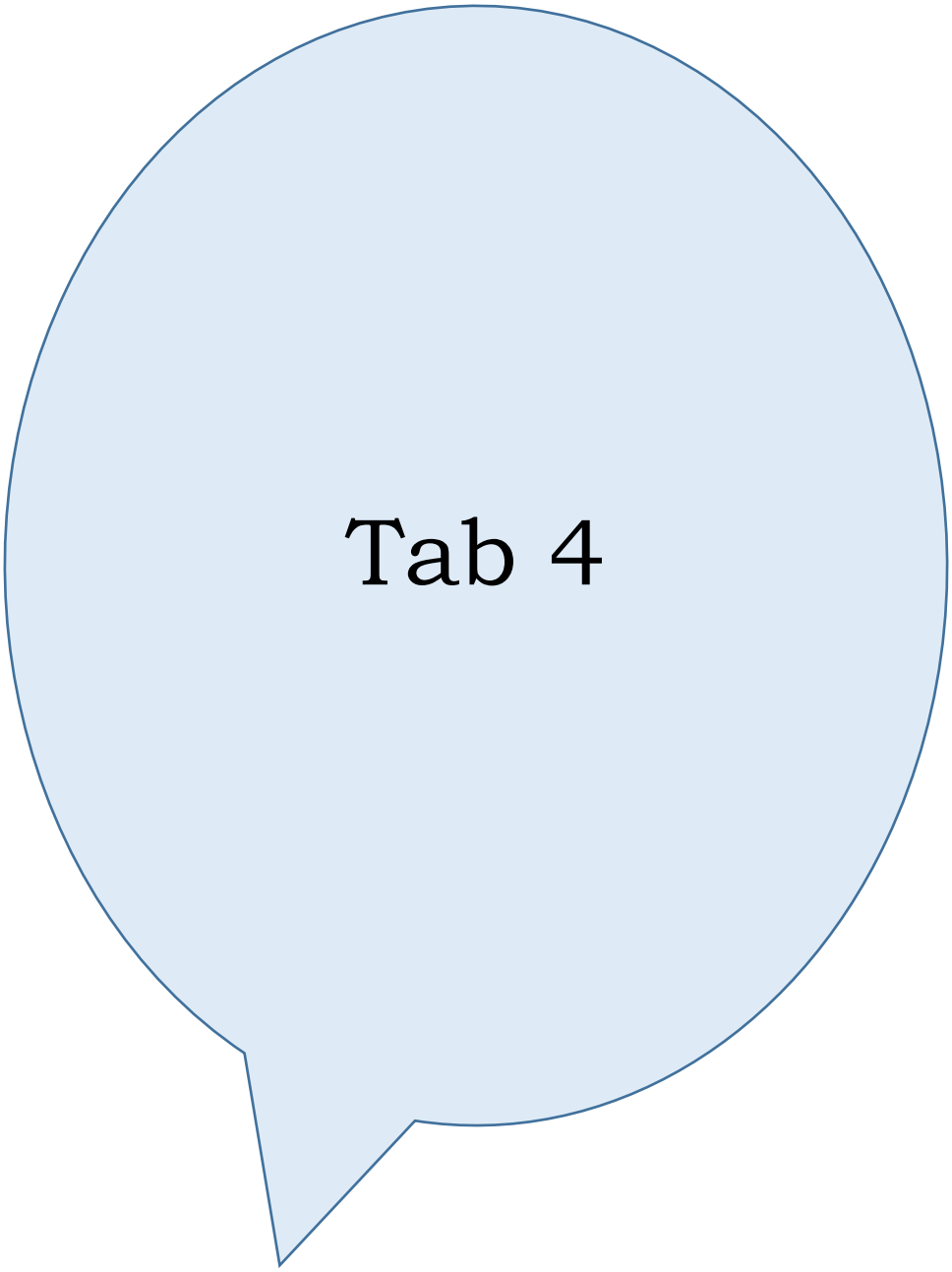

Tab 3

Risk Rating Exercise

Factor	Low	Medium	High
Nature of the personal information			
Relationship			
Cause of the breach			
Scope			
Containment efforts			
Forseeable harm			

Risk Rating Exercise

Factor	Low	Medium	High
Nature of the personal information			
Relationship			
Cause of the breach			
Scope			
Containment efforts			
Forseeable harm			


Tab 4

Insert Organization Name
Nova Scotia
Privacy Breach Management Protocol Template

Introduction:
This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. All words highlighted require consideration by the organization adapting this template for its own purposes. Sometimes the words need to be deleted (as with this paragraph) or sometimes the organization may wish to substitute words or names in place of the highlighted text (for example insert the organization's name in every place where "the organization" is mentioned). Use this document in combination with the *Key Steps to Responding to Privacy Breaches* document produced by the OIPC Nova Scotia and available at: https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf

Organization:
Date:

Author:

Index:

1. What is the purpose of the privacy breach management protocol?

The protocol allows the organization to identify, manage and resolve privacy breaches. It applies to all of the organization's information assets – such as personal information, personal health information, workforce personal information, and employee personal information. All workers at the organization must follow this protocol, including all full-time and part-time employees, contract employees, contractors, people on secondment, temporary workers and students. (municipalities should add elected officials to this list).

2. What is a privacy breach?

A breach is any event that results in personal information in the custody or control of the organization being accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, either deliberately or inadvertently.

Some examples of breaches include:

- A USB key with unencrypted personal information being lost or stolen.
- An excel spreadsheet containing employee benefit information being emailed to the wrong person.
- Employees inappropriately browsing data files containing personal information for non-work related purposes.
- Hacker engaging in malicious activity resulting in the compromise of the organization's personal information assets.

3. Roles and responsibilities

Note: Below is a sample of the positions that will have some responsibility for managing a privacy breach. Titles may vary from organization to organization and so when completing this template, insert the appropriate title for your organization. The responsibilities listed must be assigned to someone within your organization if the breach is to be properly managed. The responsibilities listed are described in more detail in the breach management process section of this document.

The following table summarizes the responsibilities of staff when a privacy breach is discovered.

Position	Responsibilities
• All staff	• Complete preliminary breach assessment report. (Appendix 1) and immediately report privacy breach to Chief Privacy Officer. • Immediately undertake containment efforts. • Assist with breach investigations as required.
• Chief Privacy Officer	• Receive preliminary breach assessment reports. • Assess the preliminary report to determine whether a privacy breach has occurred. • Recommend immediate containment efforts. • Identify and contact individuals to form an Incident Response Team. • Conduct appropriate internal notifications of the breach.

	• Conduct a full assessment of the breach – complete the privacy breach checklist (Appendix 2). • With the Incident Response Team, determine whether notification of affected individuals is required. • In consultation with communications staff, complete notification. • Notify and liaise with the Information and Privacy Commissioner. • With the Incident Response Team, identify risk mitigation and prevention strategies. • Assign responsibility for completing mitigation and prevention strategies. Follow up to ensure actions are completed. • Conduct trend analysis of privacy breaches. • Keep executive informed of all actions and decisions of the Incident Response Team.
• Chief Security Officer	• Participate on Incident Response Teams when the privacy breach involves systems. • Assist in investigations as to the cause of system-related breaches. • Identify containment and prevention strategies. • Assist in implementation of containment and prevention strategies involving IT or security resources.
• Legal counsel	• Participate as required on the Incident Response Team. • Assist Chief Privacy Officer in assessing whether notification is required.
• Communications staff	• Assist in the drafting of breach notification letters.
• Labour relations/human resources staff.	• Assist in implementation of containment and prevention strategies that require cooperation of staff, particularly unionized staff.
• Office of primary responsibility – manager or supervisor	• Participate on Incident Response Team. • Assist in identifying containment, mitigation and prevention strategies. • Implement containment, mitigation and prevention strategies.
• Executive	• Receive and review all reports of privacy breaches. • Follow up with Chief Privacy Officer to ensure that containment, notification and prevention actions have been completed.

4. Breach Management Process

Step 1: Preliminary Report, Assessment & Containment
Step 2: Full Assessment
Step 3: Notification
Step 4: Mitigation and Prevention
Step 5: Lessons Learned

Step 1: Preliminary Report, Assessment & Containment

When a suspected privacy breach occurs, the employee who discovers the breach must conduct a preliminary assessment to identify the nature of the breach and to identify potential containment steps.

Employees who discover potential breaches must:

- Immediately complete the Preliminary Breach Assessment Report (Appendix 1). The report assists employees in identifying a privacy breach and in identifying useful containment strategies. The preliminary report should be completed on the day the breach is discovered.
- Contact the Chief Privacy Officer and provide a copy of the Preliminary Breach Assessment Report on the day the breach is discovered.
- Advise their supervisor of the potential privacy breach and of steps taken to contain the breach on the day the breach is discovered.

Supervisors and employees who discover potential breaches must:

- Take immediate action to contain the breach and to secure the affected records, systems, email or websites. Review the Preliminary Breach Assessment Report (Appendix 1) for suggested containment strategies.

Step 2: Full Assessment

Upon receipt of a notification of a potential privacy breach, the Chief Privacy Officer must:

- Obtain a copy of the Preliminary Breach Assessment Report from the reporting employee (Appendix 1).
- Identify appropriate staff to form an Incident Response Team and organize an immediate meeting of the team.
- Identify breach containment strategies and assign responsibility for their implementation. Containment strategies should be identified and implemented on the day the breach is discovered.
- Conduct an investigation and complete the Privacy Breach Checklist including a risk assessment (Appendix 2). Conduct this step within one to five days of the breach.
- Based on the Privacy Breach Checklist and in consultation with the Incident Response Team, determine whether notification is appropriate and identify prevention strategies. Conduct this step within one to five days of the breach.
- Complete notification of affected individuals and notification of the Information and Privacy Commissioner. Conduct this step as soon as possible, generally within one to five days of the breach.

Step 3: Notification
The Incident Response Team, in consultation with the Chief Privacy Officer, will determine whether and to whom notification will be given. Notification is an important mitigation strategy that can benefit both the organization and the individuals affected by a breach. There are a number of individuals and organizations that may require notification:

(a) Internal officials: The Incident Response Team should identify appropriate officials within the organization who require notification of the breach.

(b) Affected individuals: If a breach creates a risk of harm to any individuals, those affected should be notified. The Privacy Breach Checklist (Appendix 2) includes an assessment for whether notification should occur and how notification should be completed. The Privacy Breach Checklist also identifies the information that must be included in any breach notification letter.

(c) Office of the Information and Privacy Commissioner
The Chief Privacy Officer will notify the Office of the Information and Privacy Commissioner by phone, fax or email.

(d) Others
Appendix 2 includes a list of other organizations or individuals who may require notification depending on the facts of the breach. The Chief Privacy Officer is responsible for implementing any notification decisions made by the Incident Response Team.

Caution: In responding to a privacy breach, be careful not to take steps that may exacerbate the existing breach or create a new one (i.e. disclosing additional personal information, notification letters addressed to the wrong person, notification letters that disclose information in the return address).

Step 4: Mitigation and Prevention
Once the immediate steps have been taken to mitigate the risks associated with the privacy breach and to provide appropriate notification, the Office of Primary Responsibility (the Office where the breach occurred), the Chief Privacy Officer and the Incident Response Team must investigate the cause of the breach thoroughly, consider whether to develop a prevention plan and consider what that plan might include.

Mitigation and prevention strategies developed should reflect the significance of the breach and whether the breach was a systemic or isolated event. Mitigation and prevention plan may include the following:

Physical Controls
- Audit physical controls to identify outstanding weaknesses.
- Modify physical controls such as locks, alarms, security monitoring, or visitor access control to improve level of security.

Technical Controls
- Tighten restrictions on access to certain personal information based on roles, responsibilities and need to know.
- Encrypt personal information particularly on portable storage devices.
- Limit the ability to copy data to thumb drives.
- Limit access to non-work email.

Administrative Controls

- Review the enforcement of the organization's policies, directives and process for the protection of personal information throughout its lifecycle.
- Revise or develop internal procedures and policies to address shortcomings identified.
- Develop contractual clauses to deal with breaches of privacy by third party service providers.

Personnel Security Controls

- Training and education
- Coaching/mentoring
- Disciplinary actions (reprimands, suspension, reassignment, termination)
- Revoke privileges and/or user access to system or records

Step 5: Lessons Learned

The Chief Privacy Officer will track all privacy breaches across the organization and will use that information to identify trends both in the types of breaches occurring and within each step of the privacy breach management process. Collecting this information can facilitate identifying underlying patters with respect to personal information handling practices and may prevent future breaches.

Appendix 1: Preliminary Privacy Breach Assessment Report	
Report Prepared by:	**Date:**
Email:	
Phone:	

A. Breach Identification and Containment

Instructions: Review the preliminary assessment list below. If you answer yes 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 Chief Privacy Officer.

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)?		a) Immediately restrict, suspend or revoke access privileges until completion of the investigation. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Attempt to retrieve the documents in question, and document the steps taken. d) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
2. Was personal information inappropriately disclosed (e.g. improper application of severances (material removed or blacked out), incomplete de-identification)?		a) Attempt to retrieve documents. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
3. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)?		a) Attempt to retrace steps and find the lost document(s). b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Conduct an inventory of the personal information that was or may have been compromised. e) Complete this *Preliminary Report* and contact the Chief Privacy Officer.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
4. Was personal information stolen (e.g. theft of computer equipment or devices)?		a) Attempt to retrieve the stolen equipment or device. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
5. Was personal information in an unencrypted email sent to the wrong address?		a) Cease transmission of email or correspondence to the incorrect address. b) Determine whether the email address is incorrect in the system (e.g. programmed incorrectly into the system). c) Attempt to recall the message. d) Determine where the email went. e) Request that the recipient delete all affected email or correspondence, with confirmation via email that this has been done. f) Determine whether personal information was further disclosed to others (verbally or via copies). g) Document the steps taken. h) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
6. Was personal information faxed, mailed or delivered to a wrong address?		a) Determine where the document went. b) Determine whether the address is incorrect in the system (e.g. programmed incorrectly into system). c) Request that the recipient return the document(s) if mailed, or request that the fax be destroyed, with confirmation that this has been done. d) Determine whether personal information was further disclosed to others (verbally or via copies). e) Document the steps taken. f) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
7. Did a third party compromise (hack into) a system that contains personal information?		a) 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. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
8. 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?		a) Contact IT. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
9. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g. posting of medical appointments or types of		a) Remove, move or segregate exposed information or files. b) Preserve evidence. c) Determine whether personal information was further disclosed to others (verbally or via copies). d) Document the steps taken.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
leave, home telephone numbers, slides of PowerPoint presentations that contain personal information, etc.)?		e) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
10. Was there an inappropriate collection of personal information?		a) Determine whether personal information was further disclosed to others (verbally or via copies). b) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
11. 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?		a) Determine whether personal information was further disclosed to others (verbally or via copies) b) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
12. Was there an improper or unauthorized creation of personal information?		a) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
13. Was there an improper or unauthorized retention of personal information?		a) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
14. Remarks/Other:		

B. Breach Details		
1. Date(s) of breach:	2. Time of breach:	3. Location of breach:
4. When and how was the breach discovered?		
5. Provide a brief description of the breach (what happened, how it happened, etc.):		
6. 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.		7. Is/are the affected individual(s) aware of the breach? __ Yes __ No Whether yes or no, request direction from the Chief Privacy Officer or the OIPC.
8. Format of information involved: ____ Electronic records ____ Paper records ____ Other (describe): _____	9. What information was involved (check all that apply): ____ Medical _____ Employee ____ Other (describe): _____	
10. List the immediate containment actions and/or interventions, if any:		
11. Is there information or evidence to support the allegation of the breach? If yes, please specify:		
12. Has your supervisor been notified of the breach? __ Yes __ No		

C. Please name the person(s) directly involved in this breach (witnesses, investigator, individual who may have caused the breach, victims, etc.). Attach a list if necessary.		
1. Name	Title/Position	Contact information:
2. How was this person involved?		
3. Name	Title/Position	Contact information:
4. How was this person involved?		

Send this form immediately to the Chief Privacy Officer at [insert contact information – email & phone #]

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.[5] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: https://oipc.novascotia.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

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

_____

_____

_____

_____

[5] The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by email at oipcns@novascotia.ca.

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 15.

(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 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:

_____

_____

_____

_____

(2) 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) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ 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 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 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)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

_____

(7) 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
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

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

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 from the breach			
7) 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

(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. 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 licence 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.	

(2) 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	

(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 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	

(4) 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:	
Technology suppliers	
Others (list):	

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,[6] and assess if any further adjustments are necessary as part of your prevention strategy.

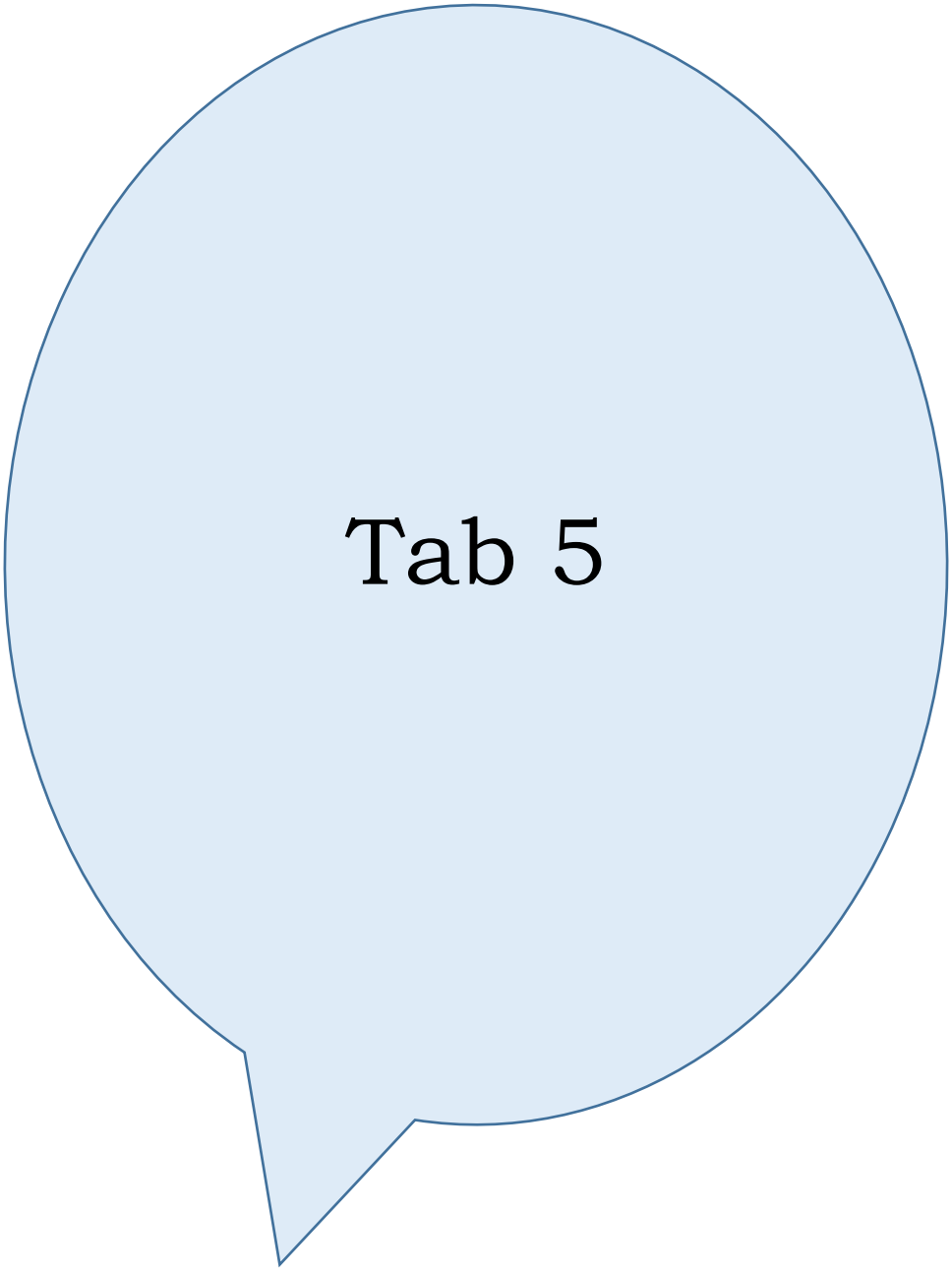
Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

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?

[6] For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner website at: https://oipc.novascotia.ca.


Tab 5

Privacy Breach Workshop
Scenario #1

Facts:
You are the Chief Privacy Officer for your organization. It's 9:45 on a Friday morning when you receive a panicked phone call from Bob, in human resources. Bob had a late night last night. After work he went out with a couple of friends. He took his work laptop with him because he's bee n working on a sticky discipline issue and figured he'd get up early and work on it at home. He left his laptop on the floor of the car and then met up with his friends. He didn't get home until the wee hours and it was not until he rolled out of bed at 9:00 this morning and went looking for his laptop that he realized that his car window was broken and the bag carrying his labour relations file and laptop were gone.

Questions:
1. List the first three things you will do in response to Bob's call.
2. What recommendations, if any, do you have for Bob with respect to containment of this breach?
3. Is this an appropriate breach to set up an Incident Response Team?

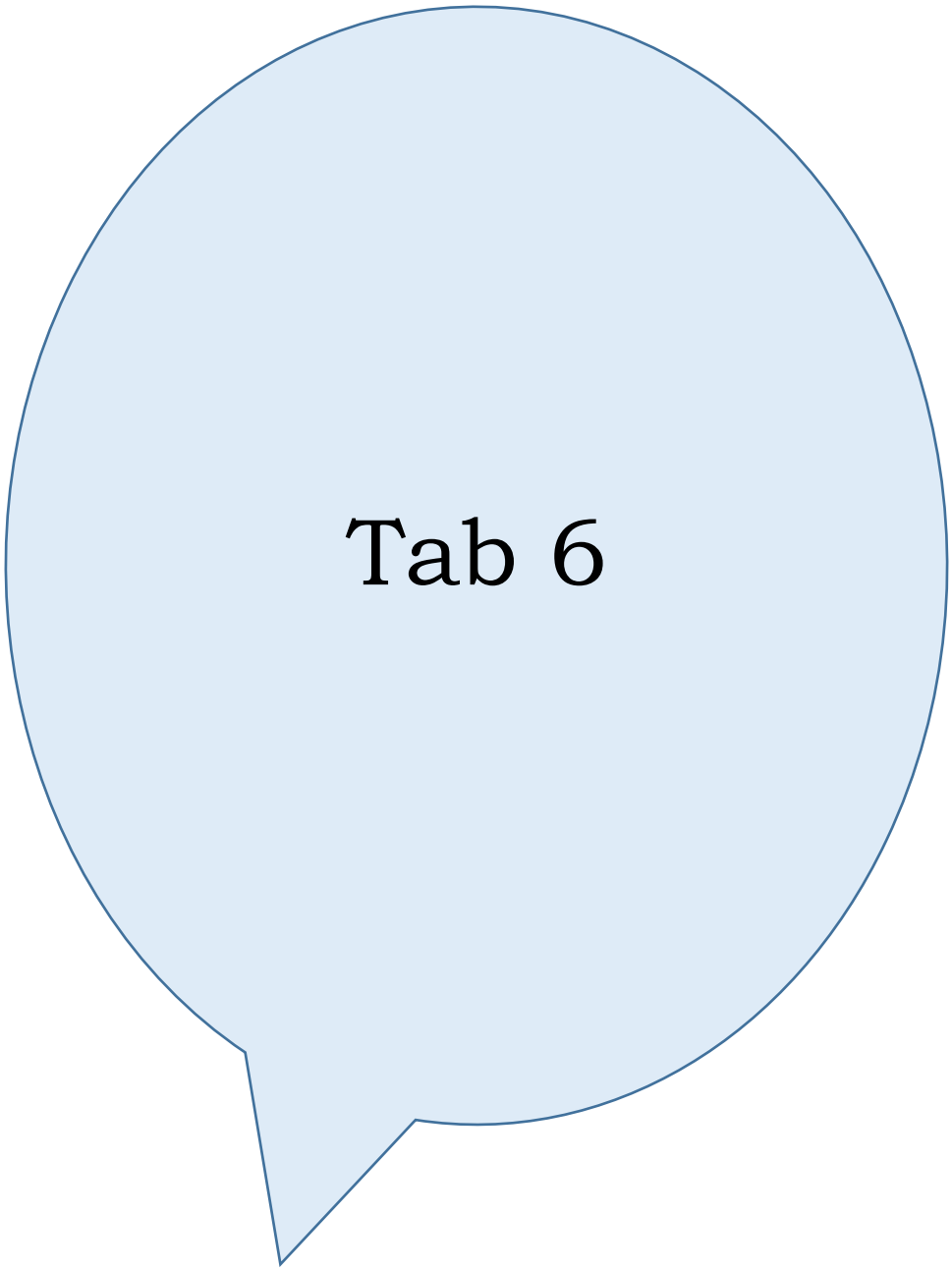
Scenario #2

Facts:
You manage a service provider for your public body. The service provider manages a billing database for your organization. The database includes the personal information of 10,000 citizens. Included in the database is name, home address, social insurance numbers, billing information, service codes, email addresses and cell phone numbers. A woman (the complainant) calls your service desk and says that she has heard that her ex-husband, who is stalking her, has found her new home address because his new girlfriend works for your service provider as an account clerk. The complainant fears for her safety and wants to know what you're going to do to help her.

Questions:

1. Is this a privacy breach?
2. Describe what containment steps, if any, you would take to manage this breach.
3. What is your assessment of the risks in this case? Complete the risk assessment table.
4. Would you provide notification and to whom?
5. What information would you include in the notification?
6. When would you notify?
7. Identify three prevention strategies you would use.

Factor	Low	Medium	High
Nature of the personal information			
Relationship			
Cause of the breach			
Scope			
Containment efforts			
Forseeable harm			


Tab 6

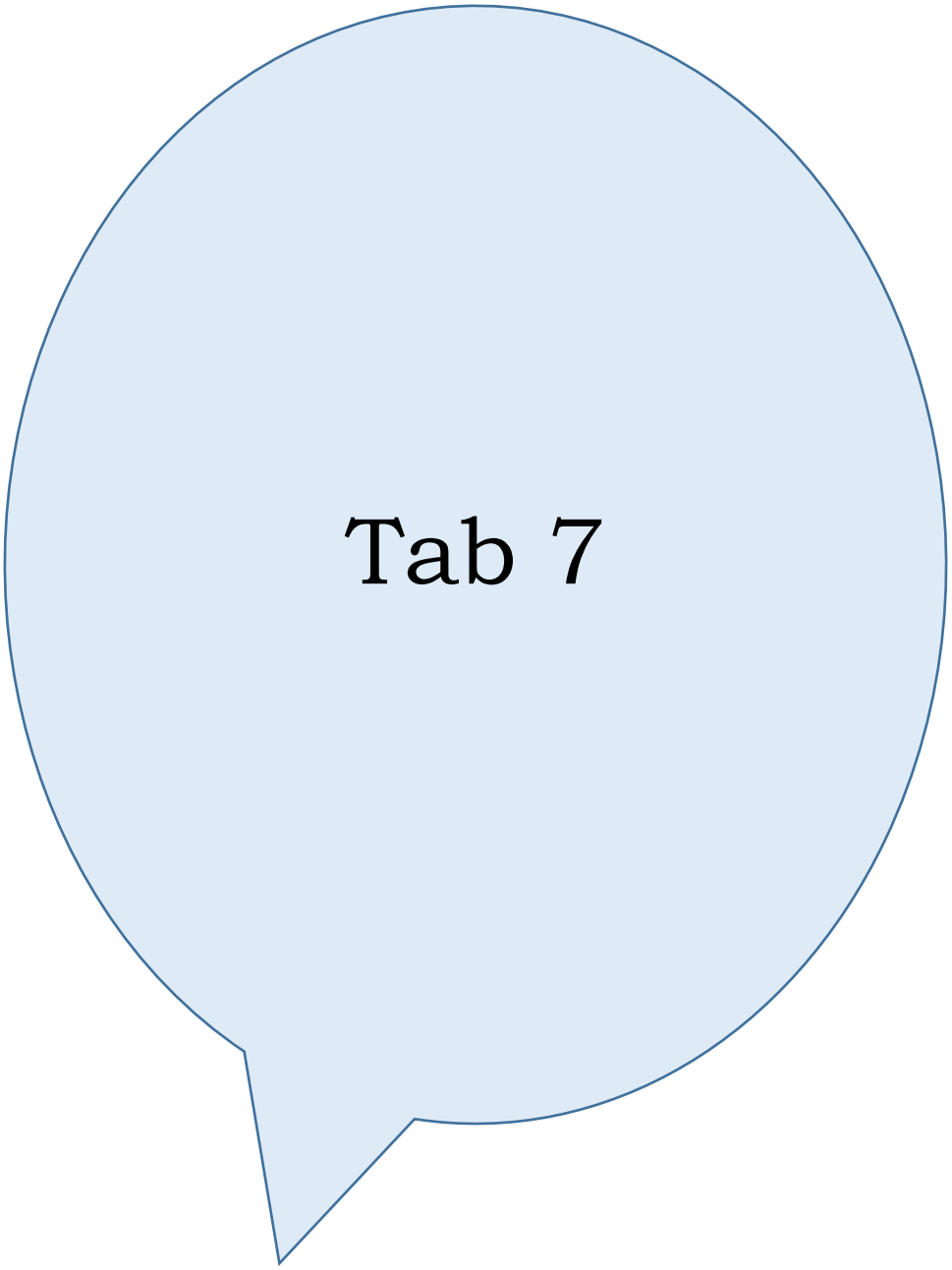
THE
5-MINUTE
PRIVACY CHECKUP

As an employee of a public body, you should be aware of your responsibilities to keep personal & sensitive information secure. Current privacy standards require that public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This 5-minute privacy checkup asks a series of questions relating to the security of personal information & sensitive business information both hard copy and electronic. A "no" answer to any of these questions is a warning sign that the information may not be secure.

Physical Security		
	Y	N
Do you have files containing sensitive information stored in your office? • If yes, is the sensitive information stored in a locked filing cabinet? • Do you lock your office door whenever you leave the office?		
At the end of the day do you always: • Clear your desktop of all files containing sensitive information? • Store your laptop and all files in a locked filing cabinet? • Lock your office door? • Log off your computer? • Remove all documents containing sensitive information from faxes and printers?		
Email & Faxing		
Before emailing sensitive information do you: • Ensure that either the owner of the sensitive information has consented to transmission via email or that the information is encrypted? • Always attach a confidentiality notice?		
Before faxing any sensitive information do you: • Only send from a secure fax machine? • Prior to sending, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number? • Always use a cover sheet that includes both the sender's name and phone number and the intended recipient's name and phone number? • Always attach a confidentiality notice?		
Security of Electronic Files		
	Y	N
Do you always have to login to any system using a unique identifier and password?		
Is your password complex (numbers, symbols, letters etc) and at least six characters in length?		

Have you changed your password in the last 90 days?		
Do you store all electronic files containing sensitive information on a secure central server? (i.e. no sensitive information stored on local hard drive)		
Is your office computer screen positioned so that no unauthorized individuals can view sensitive information displayed?		
Have you set your screen saver so that you are automatically logged out after a 5 minute period of inactivity?		
Training & Knowledge		
In the last 12 months, have you completed training on privacy and security of sensitive information?		
Do you know whether or not you have authority to collect, use or disclose personal information?		
If you do have authority to collect, use or disclose personal information, do you know the limits and conditions of that authority?		
Mobile & Portable Devices		
	Y	N
Do you always store mobile or portable storage device such as laptops in a locked cabinet when not in use?		
Is all sensitive information contained on your portable storage devices limited to the absolute minimum necessary?		
Have you ensured that all sensitive information contained on any portable storage device you use is encrypted?		
Do you permanently delete sensitive information from your portable storage devices as soon as possible after use?		
Secure Disposal of Sensitive Information		
Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?		
Privacy Habits		
Do you avoid discussing personal information in any area where the conversation can be overheard by unauthorized personnel?		
Do you disclose personal information to co-workers only where the information is necessary for the performance of the duties of your co-workers?		
If you must travel with personal information, do you always ensure that any personal information you have is stored in a locked cabinet or cupboard and never in your car?		


Tab 7

Reasonable Security Checklist

This checklist was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia.[7] Under Nova Scotia's privacy legislation, public bodies, municipalities and health custodians must all ensure that they have made reasonable security arrangements against such risks as unauthorized access to or use, disclosure, copying or modifications of personal information.[8] This checklist is intended to give a quick snapshot of some key security standards. Failure to meet the standards set out in this checklist is an indication that personal information may be at risk and that a thorough review of security should be undertaken immediately.

The checklist includes questions in each of the 17 areas of security compliance listed below and should take about 30 minutes to complete:

1. Risk Management
2. Policies
3. Records Management
4. Human Resources Security
5. Physical Security
6. Systems Security
7. Network Security
8. Wireless
9. Database Security
10. Operating Systems
11. Email and Fax Security
12. Data Integrity and Protection
13. Access Control
14. Information Systems Acquisition, Development and Maintenance
15. Incident Management
16. Business Continuity Planning
17. Compliance

[7] This document is based on "Securing Personal Information: A Self-Assessment Tool for Organizations" created by the Office of the Information and Privacy Commissioners in Alberta and British Columbia and the Office of the Privacy Commissioner of Canada. The full self-assessment tool is available at: https://www.oipc.bc.ca/guidance-documents/1439 and as an interactive tool at: https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1.

[8] *Personal Health Information Act* s. 62, *Freedom of Information and Protection of Privacy Act* s. 24(3), *Municipal Government Act* s. 483(3).

Risk Management		
	Yes	No
1. We have identified all of our personal information assets and their sensitivity.		
2. We have analyzed, evaluated and documented the likelihood of security failures occurring.		
3. We have a risk treatment plan identifying the appropriate management action, resources, responsibilities and priorities for managing personal information security risks.		
Policies		
4. We have operational security policies (such as secure faxing, end-of-day closing, use of couriers).		
5. Employees, contractors and partners have easy access to our personal information security policy.		
6. We have an acceptable use policy.		
Records Management		
7. Specific retention periods have been defined for all personal information.		
8. Personal information contained on obsolete electronic equipment or other assets is securely destroyed before the equipment or asset is disposed of.		
9. Hard copy records containing personal information is shredded, mulched or otherwise securely destroyed.		
Human Resources Security		
10. Training has been implemented for all employees, data custodians and management to ensure they are aware of and understand their security responsibilities, permitted access, use and disclosure of personal information and retention and disposal policies.		
11. All employees are required to sign confidentiality agreements.		
12. Contractors and other third parties are required to return or securely destroy personal information to the public body upon completion of the contract.		
Physical Security		
13. We have strong physical security measures for storing personal information including locked cabinets, pass cards and motion detectors or other intrusion alarm systems.		
14. Our publicly accessible service counters are kept clear of personal information.		
15. We have a nightly closing protocol that requires employees to clear personal information from their desks and lock it away, log out of all computers and remove all documents containing personal information from fax machines and printers.		
System Security		
16. All terminals and personal computers used for handling personal information are positioned so that unauthorized personnel cannot see the screens.		
17. If a user walks away from her terminal there is an automatic process to lock out all users after a short defined period of inactivity.		
18. Personal information is always stored either on a secure server or is encrypted when stored on mobile and portable devices.		

Network Security		
	Yes	No
19. We use perimeter defense safeguards including firewalls, routers, intrusion detection, anti-virus/anti-spyware/anti-malware software) to mediate all traffic and to protect systems that are accessible from the internet.		
20. All systems exposed to the internet or servers supporting sensitive applications are "hardened" (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication).		
Wireless		
21. We have a policy in place that addresses the use of wireless technology.		
22. We have enabled the strongest available security features of the wireless devices, including encryption and authentication.		
23. A wireless intrusion detection and prevention capability is deployed on our network to detect suspicious behaviour.		
Database Security		
24. Automated and/or manual controls have been implemented to protect against unauthorized disclosure of personal information.		
25. There is a formal approval process in place for handling requests for disclosure of database contents or for database access that includes an evaluation of the privacy impacts and security risks.		
Operating Systems		
26. Our operating systems are kept up-to-date with all patches and fixes.		
27. We use a regular schedule for updating definitions and running scans with anti-virus, anti-spyware, anti-malware and anti-rootkit software.		
28. We regularly check expert websites and vendor software websites for alerts about new vulnerabilities and patches.		
Email and Fax Security		
29. We regularly update our fax and email lists.		
30. All of our faxes include a fax cover sheet with sender contact information and a confidentiality notice.		
31. We do not send emails with sensitive personal information unless the recipient has consented to the use of email, the email service is secure or the email itself is encrypted.		
Data Integrity and Protection		
32. We have a procedure in place to ensure that any removal of personal information from the premises has been properly authorized.		
33. We use automated and/or manual controls to prevent unauthorized copying, transmission or printing of personal information.		
Access Control		
34. We have a role-based access control policy.		
35. We have a formal user registration process in place.		
36. Each user of our system is uniquely identified.		
37. We limit access privileges to the least amount of personal information required to carry out job-related functions.		
38. Users of our system must first be authenticated by username and unique password that is changed at least every 90 days.		

Information Systems Acquisition, Development and Maintenance		
	Yes	No
39. We always identify security requirements as part of any new system development, acquisition or enhancement.		
40. We have controls in place to prevent or detect unauthorized software.		
Incident Management		
41. We have a privacy incident management policy in place and we have assigned an individual to coordinate our response to any incident.		
Business Continuity Planning		
42. We have a backup process in place to protect essential business information.		
Compliance		
43. We regularly monitor system audit logs that relate to the handling of personal information.		
44. We maintain an up-to-date software/hardware inventory.		
45. We conduct a regular physical inventory of all portable storage devices (laptops, thumb drives, portable hard drives, cell phones).		

This document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We can be reached at:

PO Box 181 Halifax NS B3J 2M4
5670 Spring Garden Road, Suite 509, Halifax
Telephone 902-424-4684
Toll-free 1-866-243-1564
TDD/TDY 1-800-855-0511
https://oipc.novascotia.ca
Twitter: @NSInfoPrivacy