



Breach Notification Form to report under s. 70(2) of the *Personal Health Information Act*
 Send to: oipecns@novascotia.ca or Julie.Young@novascotia.ca effective July 15, 2020

Custodian:	
Custodian contact:	
Custodian file identifier #:	

1. Provide detailed, accurate and specific information about the breach:

Date breach occurred	
Date breach reported to the custodian	
Who reported the breach (job title)	
Location breach occurred (specific worksite)	
Who is responsible for the breach (job title)	
# of individuals affected (if unknown, explain)	

Describe what happened in this privacy breach	
--	--

Cause of the Breach (check the box for all that apply)		
<input type="checkbox"/>	Incorrectly addressed physical records	<input type="checkbox"/>
<input type="checkbox"/>	Correctly addressed but incorrectly delivered physical records	<input type="checkbox"/>
<input type="checkbox"/>	Staff not following procedures/protocols	<input type="checkbox"/>
<input type="checkbox"/>	Technical error (a configuration issue or technology malfunction)	<input type="checkbox"/>
<input type="checkbox"/>	PHI left unattended / unsecured	<input type="checkbox"/>
<input type="checkbox"/>	Unauthorized browsing	<input type="checkbox"/>
<input type="checkbox"/>	Other (describe):	<input type="checkbox"/>

Type of Personal Health Information affected (check the box for all categories that apply)	
<input type="checkbox"/>	Registration: name, date of birth, gender
<input type="checkbox"/>	Contact: address, email address, phone number
<input type="checkbox"/>	Unique identifier: health card number, medical record number, social insurance number.
<input type="checkbox"/>	Affiliation: ethnicity, race, family income, socio-economic status, religious affiliation, gov't agency involvement
<input type="checkbox"/>	Medical Status: treatment dates, diagnosis, date of death, infectious disease status
<input type="checkbox"/>	Biometric: images (x-ray, CT, other), DNA, fingerprint, retinal pattern, genetic information or material
<input type="checkbox"/>	Detailed Medical: lab test results, discharge information, case notes, prescription info, blood type, etc.
<input type="checkbox"/>	Other (describe):

Format of the breached information/record type (check the box for all that apply)		
<input type="checkbox"/>	Paper record	<input type="checkbox"/>
<input type="checkbox"/>	Electronic record	<input type="checkbox"/>
<input type="checkbox"/>	Electronic system. System name:	<input type="checkbox"/>
<input type="checkbox"/>	Laptop	<input type="checkbox"/>
<input type="checkbox"/>	Letter	<input type="checkbox"/>

2. How was the breach was contained?

Describe steps taken to contain the privacy breach	
---	--

Check any that apply:

- Error corrected (e.g., info sent to right person)
- The personal health information (PHI) has been recovered and all copies are now in our custody and control.
- We have confirmation that no copies have been made and the PHI has been destroyed.
- The PHI was encrypted.
- The PHI was not encrypted.
- The PHI has not been recovered but the following containment steps have been taken (check all that apply):
 - A request has been sent to the recipient to destroy the record/PHI.
 - The unit has been thoroughly searched.
 - The entire facility has been thoroughly searched.
 - The immediate neighborhood around the worksite has been thoroughly searched.
 - We have run 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.
 - Device was remotely wiped.
 - Other:

3. Provide a summary of your risk assessment for determining risk of potential for harm or embarrassment to the affected individual(s).

Describe the overall risk of harm or embarrassment to the affected individual(s) from this privacy breach. (e.g., high, medium, low)	
Describe the factors considered in reaching the overall risk assessment (e.g., containment, nature of the personal information, relationship with the individual, cause of the breach, scope of the breach, foreseeable harm from the breach, other)	
Provide the rationale for risk rating	

4. Provide details regarding follow-up, mitigation and prevention strategies:

Audit	
Training for current staff	
Training for new/future staff	
Discipline (type & position, not name)	
Technical	
Other	

5. Any other relevant information:

--