Electronic Personal Health Information
Breach Reporting Protocol

A privacy breach of electronic personal health information (e-PHI) may be identified by a physician, a staff member, a patient, or an EMR or MyHealthNS provider. Immediately upon the discovery of a privacy breach or a suspected privacy breach the following four steps must be taken:

Step 1: Contain the breach.
Step 2: Evaluate the breach and assess the risks.
Step 3: Notify and report details of the breach.
Step 4: Investigate the cause of the breach to prevent future breaches.

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.

Before continuing, ensure that you record all steps taken to investigate and manage the privacy breach. Use of the following forms may be of assistance:

Appendix A: Privacy Breach Reporting Form
Appendix B: Privacy Breach Considerations Table & Risk Reporter
Appendix C: Risk Rating Chart

Definitions

Patient. In this document, this term means either the personal health record (PHR) account holder, or a substitute decision maker who is legally authorized to decide on behalf of another person who lacks capacity to make the specific health-related decision under consideration.

Primary physician. The physician deemed most responsible for the patient who owns the PHR profile. In most cases, this will be the physician who invited the patient to use the PHR.

Privacy breach. Intentional or unintentional unauthorized access to, or collection, use, disclosure, modification or disposal of electronic personal health information (e-PHI) that may result in the loss of custody or control over e-PHI.

Responding physician. The physician to whom the breach was initially identified. This physician is responsible for ensuring execution of the breach protocol. If the privacy breach was identified to more than one physician, the physicians must decide among themselves who will be the responding physician.

Staff. Non-physician member(s) of a physician's practice who has responsibilities associated with the management/handling of e-PHI and access to the PHR.

Step 1: Contain the Breach

If a privacy breach is suspected, the Responding Physician should conduct an initial assessment of the event, focusing on answering the following questions:

- Did an inappropriate collection, use or disclosure of e-PHI occur?
- Does e-PHI continue to be at risk?
- Is there a possible violation of policy or law?

The answers to these questions will determine whether a privacy breach has occurred.

Breach Containment: If a privacy breach has been confirmed, containment should be initiated immediately in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of information.

Examples (not exhaustive) of how to contain a breach include:

- Isolate or suspend the activity that led to the privacy breach.
- Take immediate steps to recover the personal information, records or equipment from all sources, where possible.
- Determine if any copies have been made of personal information that was breached and recover/destroy the copies where possible.
- If an email/message was sent to the wrong person, physician/staff must call the recipient and ask them to securely destroy any printouts made and delete the system.
- If an unauthorized person has or may have access to the e-PHR, notify McKesson, who can disable accounts or change passwords.

Initial Investigation: The Responding Physician should investigate to understand the circumstances that led to the breach, and to ensure that all efforts to contain the breach have been completed. Any evidence revealed during the investigation must be preserved.

The **Privacy Breach Reporting Form** (Appendix A) is offered to help guide the investigation and document efforts made by the Responding Physician. It may also help identify who should be notified of the breach.

Investigation and documentation should be completed within 48 hours of breach identification. If the investigation continues beyond that time period, Step 4 should be implemented simultaneously.

Step 2: Evaluate the Breach and Assess the Risks

It is critical to understand as quickly as possible:

- what e-PHI was breached
- the scope of the breach
- who is affected, and
- the consequences that are likely to arise for the affected individual(s) as a result of the breach.

The **Privacy Considerations Table** (Appendix B) is offered as a helpful tool to identify and record information about all factors that should considered. The answers to the questions are critical in fully understanding all that is involved in the breach, including the cause and extent and, most importantly, how those impacted could be harmed.

This information will guide who, if anyone should be notified of the breach.

Step 3: Notify and Report Details of the Breach

The Responding Physician should notify any physicians who are identified as Primary Physicians on any affected patient profile(s). This notification should include:

- a description of the breach
- a summary of the containment efforts, and
- if the breach has the potential to harm or embarrass any individual(S), a request that the Primary Physician(s) notify their patient(s) directly.

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

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. The **Privacy Considerations Table & Risk Reporter** (Appendix B) is offered as a helpful tool to identify and record information about all factors that should considered.

The Responding Physician should also notify:

- the police if the breach involves theft or other criminal activity
- McKesson and request remedial action as appropriate (e.g., “unmerge” of patient profiles), and
- The Office of the Information and Privacy Commissioner (OIPC) if the breach is not notifiable as set out above (i.e., not likely to cause a patient harm or embarrassment).

<u>Extraordinary circumstances for consideration before reporting:</u>

If the police have been notified of the breach, the Responding Physician should determine from them whether notification should be delayed so that a criminal investigation is not impeded.

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 Primary Physician give the notice in person or waiting until any immediate danger has passed.

In every instance, 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. In certain cases, using multiple methods of notification, may be the most effective approach.

Step 4: Prevention of Further Breaches

Once the immediate steps are taken to mitigate the risks associated with an e-PHI breach, the Responding Physician and the Primary Physician should decide who is most appropriate to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security.

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

- physical
- technical
- administrative
- personnel

Further Resources

In the preparation of this document, Doctors Nova Scotia has relied heavily on information provided by two sources:

- The Nova Scotia Government Information Access and Privacy Services
- The Office of the Information and Privacy Commissioner

The two organizations have detailed information and tools that can be accessed online at:

- The Nova Scotia Government Information Access and Privacy Services – https://beta.novascotia.ca/documents/manage-privacy-breach-protocol-and-forms
- The Office of the Information and Privacy Commissioner – https://oipc.novascotia.ca/PHIA_Custodians

Appendix A
Privacy Breach Reporting Form

The purpose of this form is to document the theft, loss or unauthorized access, use, disclosure, copying or modification of an individual's Electronic Personal Health Information (e-PHI).

Investigation of the breach

Outline all information related to the investigation of the breach, including what e-PHI was breached and how the breach occurred. Attach all relevant documents.

Notification

Please Complete the Breach Considerations Table and Risk Reporter to assist in determining the severity of the breach and who should be notified.

Determination of whether notification is required

Will notification be made to the affected individual(s)?

[ ] Yes

[ ] No

If "**Yes**," outline how the notification will occur (e.g., phone call, letter), and by whom. Attach all relevant documents.

Notification – Individual

Include all relevant information including date and time of notification to the individual, and detailed notes of all discussions. Attach all relevant documents.

Follow-up

Outline any follow-up requested by the individual(s) or committed to by the person notifying the individual(s).

If "**No**", outline the rationale for not notifying the individual. Include information on who participated in the decision. Attach all relevant documents.

Notification: Office of the Information and Privacy Commissioner (OIPC)

If the decision has been made not to notify the affected individual(s), section 70(2) of the *Personal Health Information Act* (PHIA) requires that the Privacy Officer be notified as soon as possible. Notification could be by either the Reporting Physician or the Primary Physician. Attach a copy of the notification to the OIPC.

Appendix B
Privacy Breach Considerations Table & Risk Recorder

This document is part of the Electronic Personal Health Information (e-PHI) Privacy Breach Protocol and is designed to support the decision-making activities that occur in response to a breach. The Responding Physician can use the **Considerations Table** to help organize and summarize relevant and important elements/factors of the privacy breach.

Brief description of breach:

Physicians involved: Primary

_____ _____
_____ _____
_____ _____

Date breach occurred: Date table completed:

Table completed by:

Use this table to document relevant and important elements/factors of the privacy breach (risk analysis).

Consideration	Particulars	Check all that apply
Type of personal information breached	Relevant demographics (age, date of birth, sex, sexual orientation, marital or family status)	
	Identifying number or symbol (SIN, health card number, driver master number)	
	Financial information (banking, credit, income, debit/credit card number)	
	Medical information, including physical or mental disability	
	Other (please describe):	
Scope of breach	Number of individuals affected or potentially affected	
	Length of time from the breach to its discovery	
	Number of known or potential recipients of the PHI	

	Number of times the PHI was breached	

Consideration	Particulars	Check all that Apply
Method of breach	Electronic system access	
	Verbal disclosure	
	View only	
	Fax	
	Email/electronic transfer	
	Lost/stolen	
	Incorrect mailing address	
	Social media	
	Hacking	
	Laptop	
	USB	
Recipient(s)	Agent/employee of the medical practice	
	Another physician	
	Unauthorized family member	
	Media	
	Regulated health professional	
	Individual member of the general public	
	Multiple members of the general public	
	Unknown (lost/stolen)	
	Friend or acquaintance	
Circumstances	Unintentional access or disclosure	
	Intentional access/use without authorization	
	Intentional disclosure without authorization	
	Loss	
	Malicious intent	
	For personal gain	
	Theft (targeted)	
	Theft (untargeted)	
	Existing relationship between person who breached information and the breach subject	
Disposition (what happened to the information after the breach)	View only with no further access or disclosure	
	Returned in full	
	Confirmation of proper destruction in timely manner (e.g., shredded, deleted)	
	Unable to retrieve electronically or in paper	
	Unsure of location of information	
	Re-disclosed (e.g., to media, social media, another person)	

Safeguards	Data encrypted	
	Password protected	
	Password protected but easily overwritten	
	No controls	
	PHI requires specialized knowledge to interpret	
Foreseeable harm to affected individual(s)	Hurt, humiliation, damage to reputation associated with the loss of the personal health information	
	Identity theft or fraud - most likely when the breach includes the loss of SIN, credit card numbers, driver's licence number, debit card information, etc.	
	Physical harm - when the loss of information places any individual at risk from stalking or harassment	
Anticipated impact(s)/ burden(s) of notification to the medical practice	Resources – human	
	Resources – financial	
	Implications for (future) "trust" in health professionals/organization	

Risk Analysis Chart

Use this table to document your analysis against the **Risk Rating Chart** (Appendix C).

Factor	Low	Medium	High
Nature of the personal relationship			
Relationship			
Cause of the breach			
Scope			
Containment efforts			
Foreseeable harm from the breach			
Total			

Appendix C
Risk Rating Chart

The **Risk Rating Chart** can be used as a guide to determine what the level of risk may be. Generally, if a breach falls into the medium or high category, then most likely it will be necessary to notify the affected individuals. Use the **Risk Analysis Chart** in Appendix B to record the results and determine if notification to the affected individuals should occur.

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 medical practice that is not medical or financial information.	Medical, psychological, counselling, or financial information or unique government ID 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, neighbours 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.
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.	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	Data was not encrypted. Data, files or device have not been recovered. Data at risk of further disclosure particularly through mass media or online.

	Hard copy files or device was not accessed prior to wiping. Hard copy files or device were recovered almost immediately, and all files appear intact and/or unread.	but sufficient time passed between the loss and recovery that the data could have been accessed.	
Foreseeable harm from the breach	No foreseeable harm from the breach.	Hurt, humiliation, damage to reputation or relationships. Social/relational harm. Loss of trust in the medical practice	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.

Appendix D
Contact Information

Doctors Nova Scotia
25 Spectacle Lake Drive
Dartmouth, NS
B3B 1X7
Phone: 902-481-4921
Email: nancy.milford@doctorsns.com

Information Access and Privacy Services
NS Department of Internal Services
5161 George Street, 12th Floor, Suite 1201
Halifax, NS
B3J 1M7
Phone: 902-424-2985
Email: iapservices@novascotia.ca

McKesson (RelayHealth)
Phone: 1-855-349-8333
Email: support@relayhealth.ca

Office of the Information and Privacy Commissioner
509-5670 Spring Garden Road
Halifax, NS
B3J 1H6
Phone: 902-424-4684
Email: oipcns@novascotia.ca