

PHIA Basics for staff

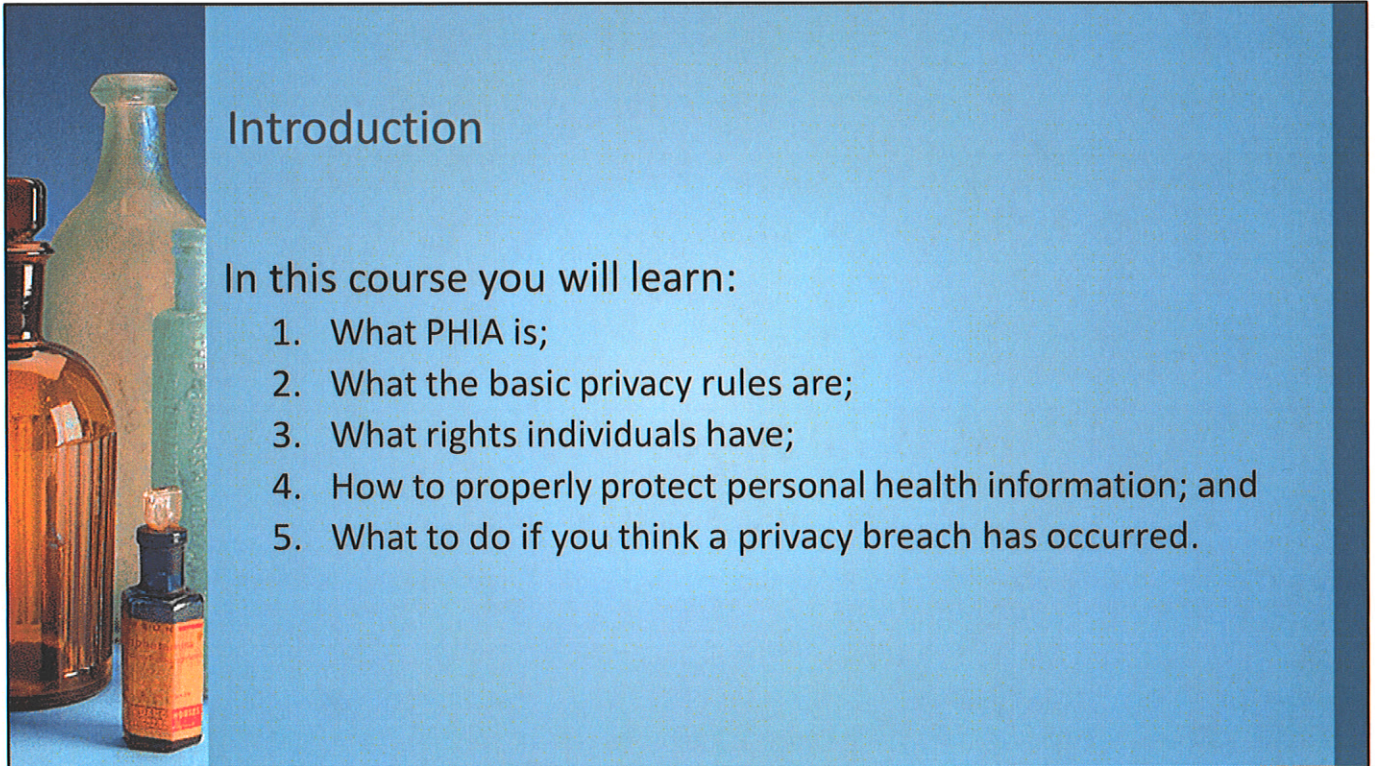
Protecting Personal Health Information

December 2019

Note to presenter-

The following pages include speaking notes. Text in **red** indicates a recommendation to insert a name or other text before using this presentation.

This deck was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. All images are used with permission for the sole purpose of illustrating this presentation.



Introduction

In this course you will learn:


1. What PHIA is;
2. What the basic privacy rules are;
3. What rights individuals have;
4. How to properly protect personal health information; and
5. What to do if you think a privacy breach has occurred.

This 30 minute presentation is intended to provide staff with some very basic information about the access and privacy law for personal health information in Nova Scotia.

You will learn some of the basic rules and what your obligations as a staff member (agent) are.

If you have questions or concerns you should speak to **{insert contact name here}**, the privacy officer for **{insert your organization's name here}**.

We are subject to the access and privacy rules in the Personal Health Information Act- we will refer to this as PHIA.



Our Privacy Program

Insert information here about:

-who your privacy lead is

-what your privacy program is made up of (training, policies, practices, advice, auditing, investigations)



1. What is PHIA?

1. What is PHIA?

- › PHIA is the *Personal Health Information Act*
- › A provincial law that governs health custodians
- › Sets privacy rules
- › Sets information protection standards
- › Gives citizens the right to complain
- › Creates offences

-{insert FN name} is a health custodian

-we must abide by the privacy rules in PHIA

-rules say we can only collect, use or disclose personal health information as set out in the law

-rules say we must have certain policies and processes in place to protect personal health information

-citizens are given rights, including the right to complain to the privacy commissioner if they think we have violated these privacy rules

-there are offences in the law for willfully contravening the rules and for failing to protect personal health information



2. What are the basic privacy rules?

Custodians & Agents

- › Privacy rules apply to “custodians” and “agents”
- › Privacy rules apply to “personal health information”



The law applies to “custodians” and “agents” treatment of personal health information

Custodians include:

- Regulated health professionals
- Pharmacies
- Continuing care facilities
- Mi'kmaw First Nations listed in PHIA regulations

Agent means:

- a person authorized by the custodian to provide health care related services.
- Agents include employees and volunteers.

Personal Health Information

Personal health information means:

- › information about an individual
- › living or deceased
- › recorded or unrecorded
- › that relates to:
 - physical and mental health
 - eligibility for and provision of health care
 - registration information including health card number



“personal health information” means:

- Identifying information about an individual
- Recorded and unrecorded
- Includes physical or mental health information, family history, information that relates to eligibility and provision of health care and registration information

this includes the fact that someone has sought treatment

this includes the identity of an individual's health care provider

We often refer to it as just 'PHI'.

The basic privacy rules:

› No collection, use or disclosure of personal health information unless:

- The individual consents and
- The collection, use or disclosure is reasonably necessary for a lawful purpose

Or

- The collection use or disclosure is permitted or required by law



The basic rule is that you must have the consent of an individual to collect, use or disclose personal health information.

But consent is not enough. The collection, use or disclosure must also be reasonably necessary for a lawful purpose.

For example, it is not considered reasonably necessary for a lawful purpose for a health care worker to look up her sister's health information even with the sister's consent if the health care worker does not have a need to know the health care information for work purpose and is not providing care to her sister.

Likewise, it is not lawful to look up your own personal health information because while you can consent to such a look up, the collection of your own personal health information is not reasonably necessary for a lawful purpose – because you are not responsible for providing your own health care.

Three best practices:

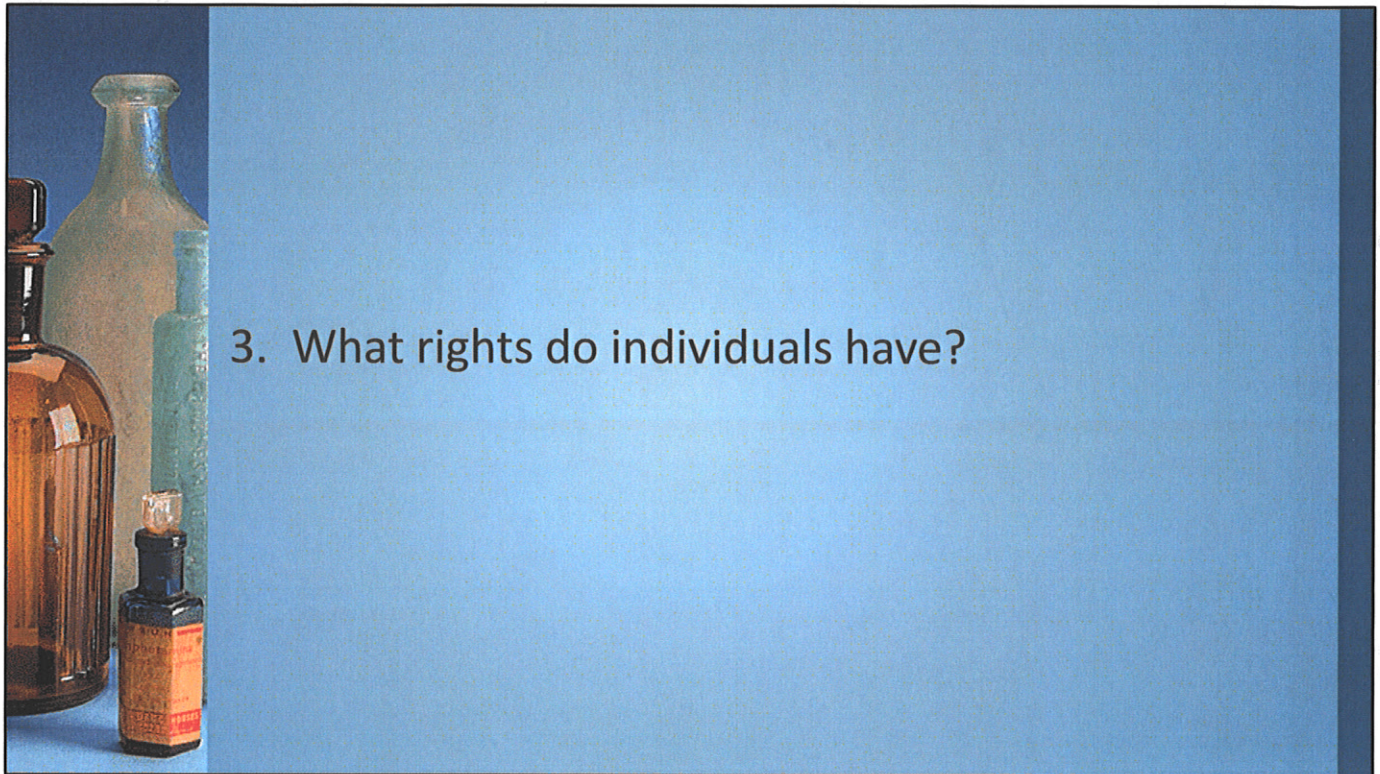
Best practice requirements:


- Non personal information first
- Minimum personal health information necessary
- Need to know



The law requires that custodians:

- Shall not collect, use or disclose personal health information if other, non-personal information will serve the purpose
- Collection, use or disclosure of personal health information must be limited to the minimum amount necessary
- Use and disclosure of phi 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





3. What rights do individuals have?


- Right to a copy of PHI
- Right to record of user activity
- Right to mask information
- Right to complain

Individuals are entitled to ask for and receive a copy of their own personal health information.

Individuals are also entitled to know who has viewed their personal health information. A record of user activity provides information about who access personal health information, how often and when.

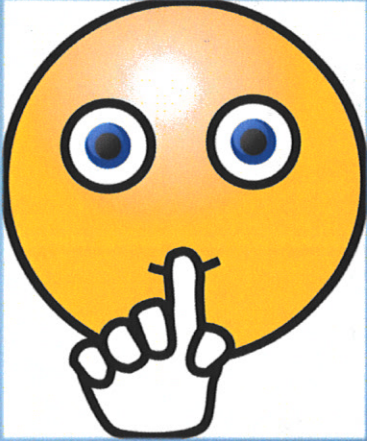
Individuals can limit or revoke consent. For example, individuals can request that identified health care providers not be permitted view certain personal health information. This is known as “masking”.

If individuals believe that either their access or privacy rights have been violated, they can complain to the Office of the Information and Privacy Commissioner. The Commissioner will investigate these complaints.



Privacy rules for staff

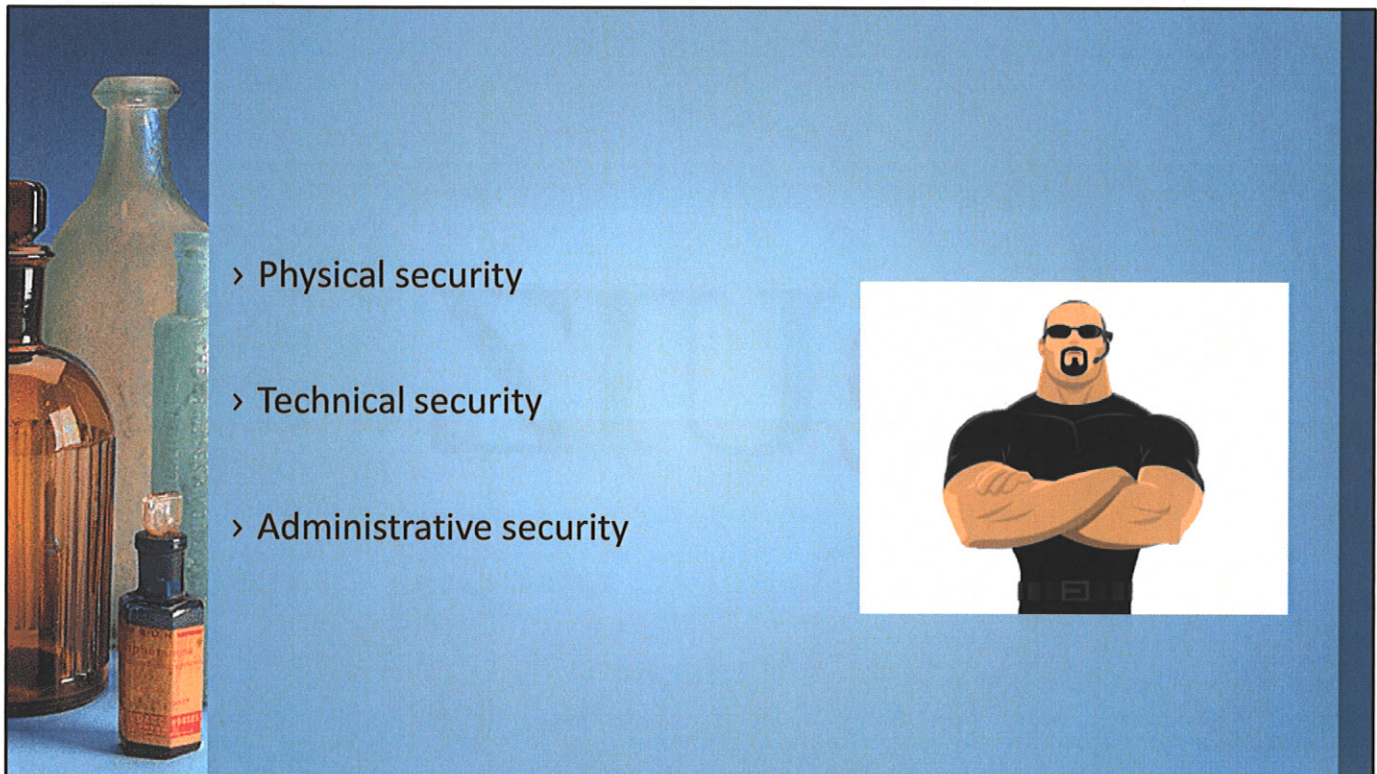
- › Know the privacy rules that apply to your work
- › Use privacy impact assessments
- › Keep personal information secure



- If your work involves the use of personal health information be sure you know exactly what information you are authorized to collect, use and disclose:
 - Only collect, use or disclose personal information if **necessary** for your work
 - Always collect, use or disclose the minimum necessary
 - Only share PHI with coworkers if it is necessary for them to do their work
 - Only access PHI on systems if it is necessary for your work
- If you are planning a new project, program or system that will involve personal health information, conduct a privacy impact assessment (PIA) to identify and mitigate your privacy risks.
- PIA templates are available at: <https://oipc.novascotia.ca/>
- You must keep personal information secure.



4. How to protect personal health information



- › Physical security
- › Technical security
- › Administrative security

Physical security

Locks, security systems, pass cards

Technical security

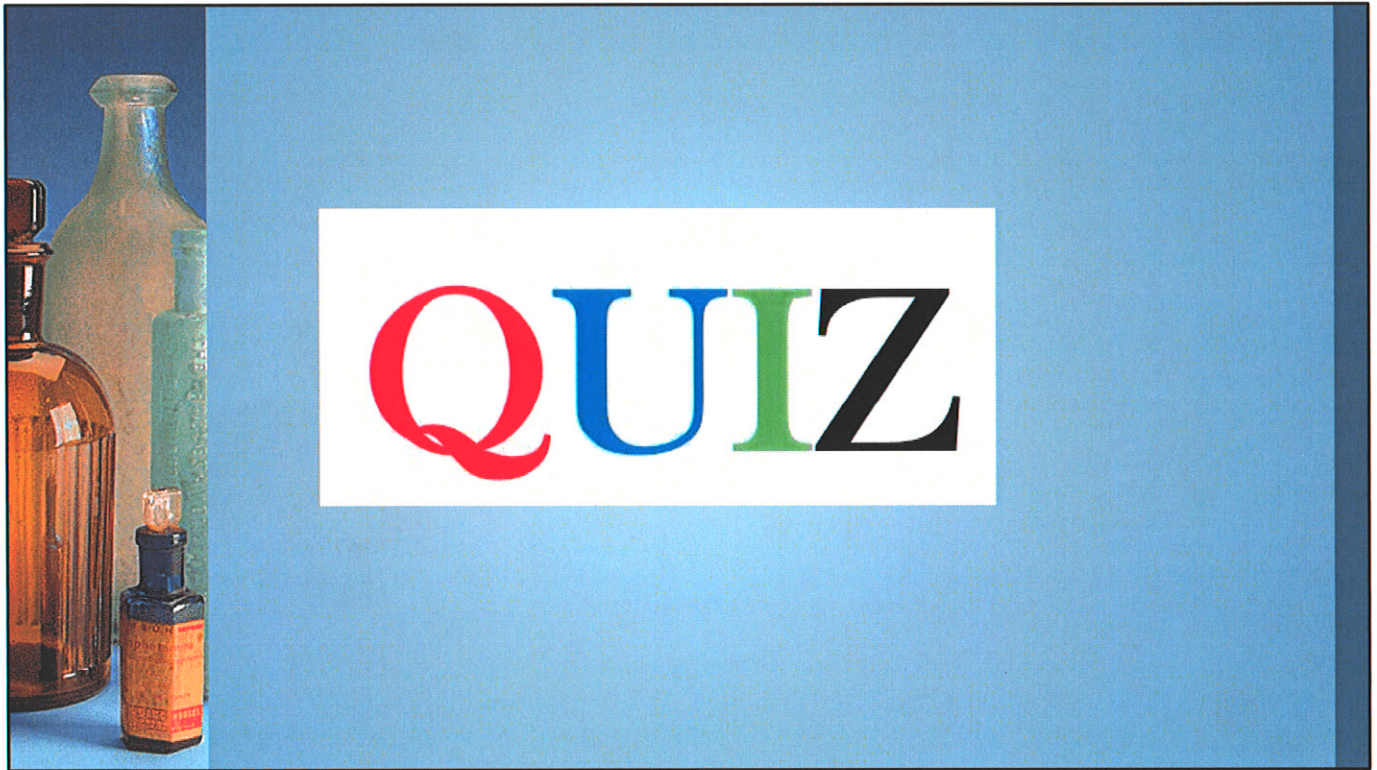
Passwords, encryption, unique user names & passwords.

Only use devices controlled by the public body or only devices with security equivalent or superior to the public body's systems

Administrative security

End of day procedures – clear desk, lock all cabinets, clear all photocopiers, log out of all systems

Travel procedures – no unencrypted personal information, take minimum necessary, remove all personal information from devices upon return

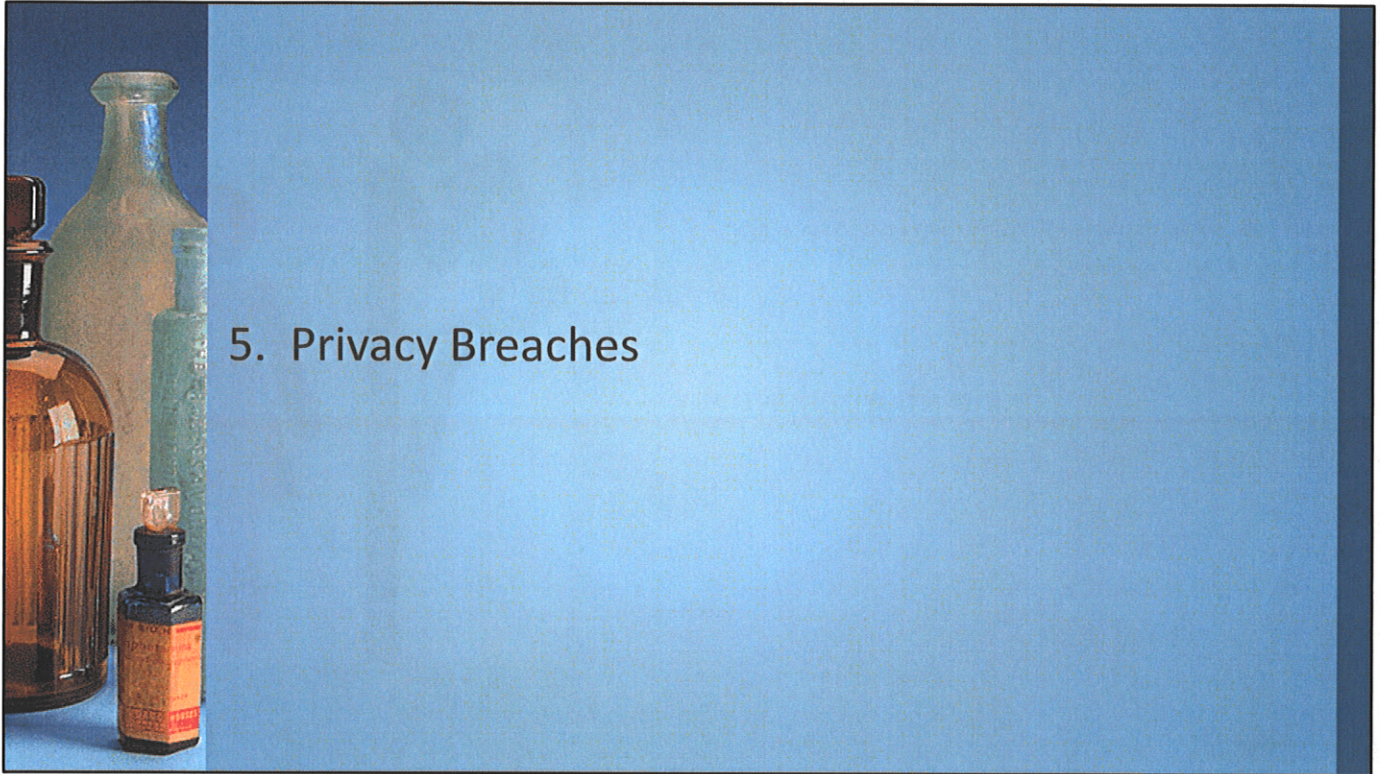


Are you keeping personal information reasonably secure?

Note to presenter: Hand out the 5 Minute Privacy Check Up

Take a few minutes to complete the 5 minute privacy check up. Think only about personal health information you have – on your computer, in your office or in your work area. Think about your personal privacy practices as you answer this quiz.

Any “no” answer is a red flag – think about how you can get your answer to “yes”.



WHAT IS A PRIVACY BREACH?

1. Must involve personal health information
2. Must be an unauthorized activity
 - collection
 - use
 - access
 - disclosure
 - destruction



To know if a privacy breach has occurred ask three questions:

1. Was any personal health information involved?
2. Was the personal health information collected, used, disclosed, accessed, or disposed of?
3. Was the activity authorized under Nova Scotia's personal health information law?

Examples of privacy breaches

- Stolen laptop or portable storage device with personal information stored on it
- Mis-sent fax or email
- System hack
- Insecure disposal of personal health information (e.g. clinical notes in non-secure garbage)
- Unauthorized viewing of database records (e.g. looking up your co-worker's birthday)



Consider the situations listed on this slide. Are any of these situations a privacy breach? How do you know?

All of the situations are potential privacy breaches.

Every situation appears to be an unauthorized loss of information – either through error or theft.

In the fax, email and systems hack situations you must establish if any personal health information was at risk (highly likely).

All of the other situations make clear personal information was at risk.

Harder to spot breaches

1. Your daughter sat in your office while you completed a few patient chart entries.
2. You left those patient charts out on your desk overnight so you can get back to work on them in the morning.
3. You post work party pictures on Facebook.



1. If your daughter could see your computer screen (or paper file) this is an unauthorized disclosure. If your daughter could overhear any discussion you had about patients, this is also an unauthorized disclosure.

Best practice: have her wait in the waiting room.

2. Personal health information sitting on a desk is not reasonably secure, particularly if you do not lock your office door. Personal health information on a desk even in a locked office is not secure if cleaning staff access your office after hours.

Best practice: ensure your desk is clean and all personal health information is locked away at the end of the day.

3. Posting of pictures is a disclosure. You should have the consent of your co-workers to post their images. If you've capture images of patients, patient files or screen shots of patient profiles, you will need the express consent of the patient to post the picture (see s. 43 of PHIA) - it is unlikely that the disclosure is reasonably necessary for a lawful purpose.

What to do if a privacy breach occurs

Step 1 – Contain the breach

Step 2 – Call the Chief Privacy Officer

Step 3 – Assist in the investigation as requested



{Note to presenter – if you've adopted a privacy breach protocol, adapt this slide to reflect this and hand out the protocol}

Step 1 – Immediately take steps to contain the breach. For example, attempt to retrieve lost or stolen documents (e.g. if a device is stolen immediately change passwords, send remote kill if possible).

Step 2 – Call **{insert Chief Privacy Officer's name here}**. This is the person responsible for managing privacy breaches in our organization – if you don't know who to call, immediately call your manager.

Step 3 – Assist with the investigation as requested.

For more information see *Key Steps to Responding to Privacy Breaches* at https://oipc.novascotia.ca/PHIA_Custodians

