SOR-RL Privacy Training - Transcript

Module 1: Introduction

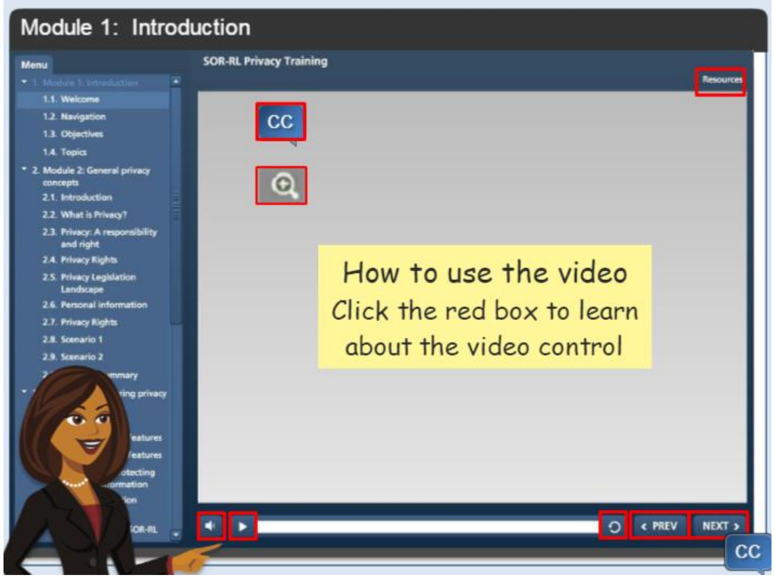
Welcome

Serious Occurrence Reporting and Residential Licensing System
SOR-RL
Privacy Training
If you can't hear me, please check your speakers
CC

Hello and welcome to the Serious Occurrence Reporting and Residential Licensing System privacy training video.

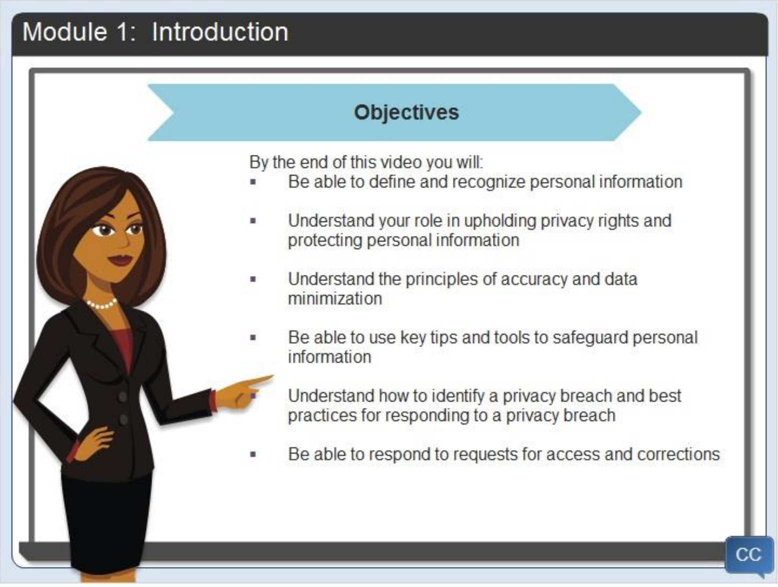
My name is Lisa. In this video I will introduce you to basic concepts about privacy, tips and tools you can use in your day-to-day work to support privacy practices. We will cover several topics including privacy rights and responding to privacy breaches.

Navigation



Take a minute to become familiar with the video controls. Just click the red boxes to learn more. Click the next button when you are ready to begin.

Objectives



Module 1: Introduction

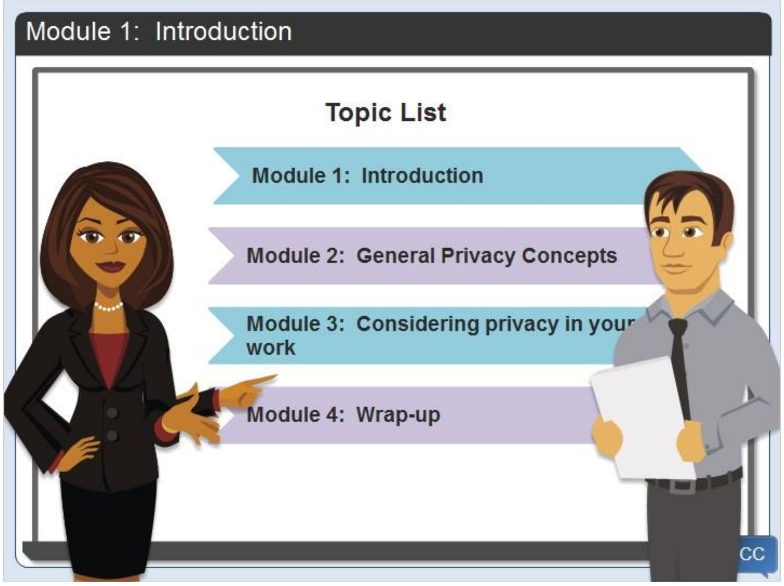
Objectives

By the end of this video you will:

- Be able to define and recognize personal information
- Understand your role in upholding privacy rights and protecting personal information
- Understand the principles of accuracy and data minimization
- Be able to use key tips and tools to safeguard personal information
- Understand how to identify a privacy breach and best practices for responding to a privacy breach
- Be able to respond to requests for access and corrections

Take a minute and review the objectives of this video.

Topics



Module 1: Introduction

Topic List

Module 1: Introduction

Module 2: General Privacy Concepts

Module 3: Considering privacy in your work

Module 4: Wrap-up

The presentation is made up of modules. Here is a brief overview of what we will be covering in each module.

We're currently in module 1.

In module 2 I'll review general privacy concepts.

Then in module 3 I'll focus on considering privacy in your work, emphasizing how privacy concepts have been incorporated into SOR-RL.

In the final module I'll do a brief summary and talk about next steps.

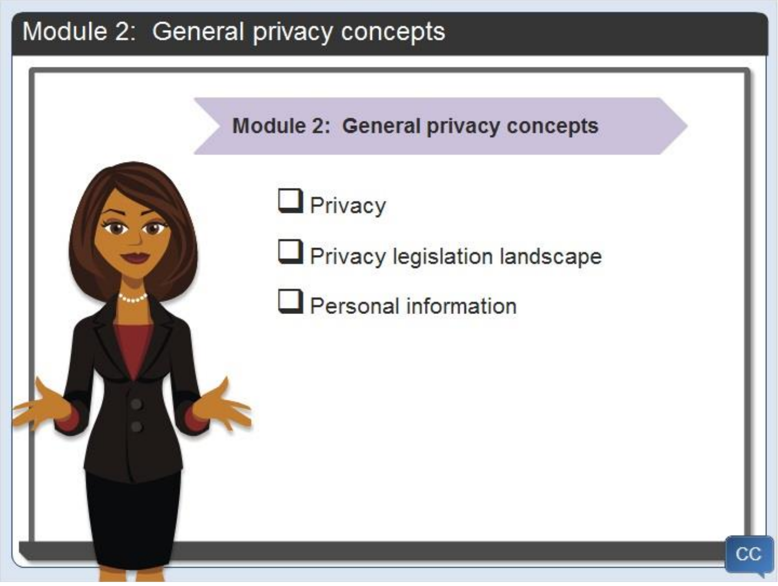
Robert: Hi Lisa. My name is Robert. I'd like to learn more about privacy and I hope it's ok for me to sit in.

Lisa: Welcome Robert. Just let me know if you have a question.

We have a lot to explore …so let's get started!

Module 2: General privacy concepts

Introduction



Module 2: General privacy concepts

Module 2: General privacy concepts

□ Privacy

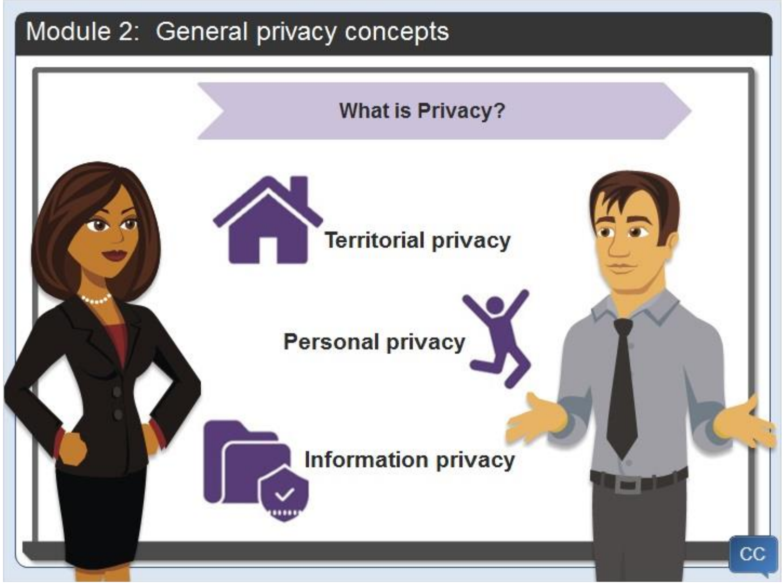
□ Privacy legislation landscape

□ Personal information

In module 2 we will look at general privacy concepts.

By the end of this module, you will be able to:
Define privacy and identify the importance of protecting privacy of personal information.
Identify and describe the current environment of privacy legislation in Ontario.
And define and recognize personal information.

What is Privacy?



Module 2: General privacy concepts

What is Privacy?

Territorial privacy

Personal privacy

Information privacy

Lisa: What do you think of when you hear the term “privacy”?

Robert: I think privacy has different dimensions.

Lisa: It sure does Robert. Tell me more.

Robert: Privacy has three dimensions:

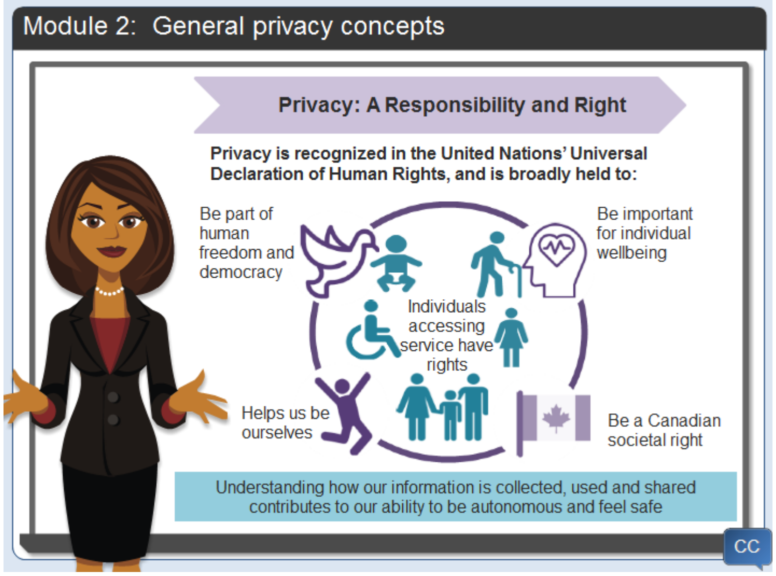
The first one is territorial privacy. It includes space or a location free from intrusion and is historically related to your home.

The next one is personal privacy, which includes freedom of movement and expression and the right to personal space.

The last one is Information privacy. This type of privacy provides individuals with control and ownership over their own personal information such as medical history, birth dates and banking information.

Lisa: Thanks for that very complete definition Robert. In this training I’m going to focus on information privacy where individuals determine when, how and to what extent information about themselves is collected, used or shared.

Privacy: A responsibility and right



Module 2: General privacy concepts

Privacy: A Responsibility and Right

Privacy is recognized in the United Nations' Universal Declaration of Human Rights, and is broadly held to:

Be part of human freedom and democracy
Be important for individual wellbeing
Individuals accessing service have rights
Helps us be ourselves
Be a Canadian societal right
CC

Understanding how our information is collected, used and shared contributes to our ability to be autonomous and feel safe

As technology advances, our privacy is more important than ever. Privacy is a part of human freedom and democracy, important to individual wellbeing, helps us be ourselves, and is a Canadian societal right.

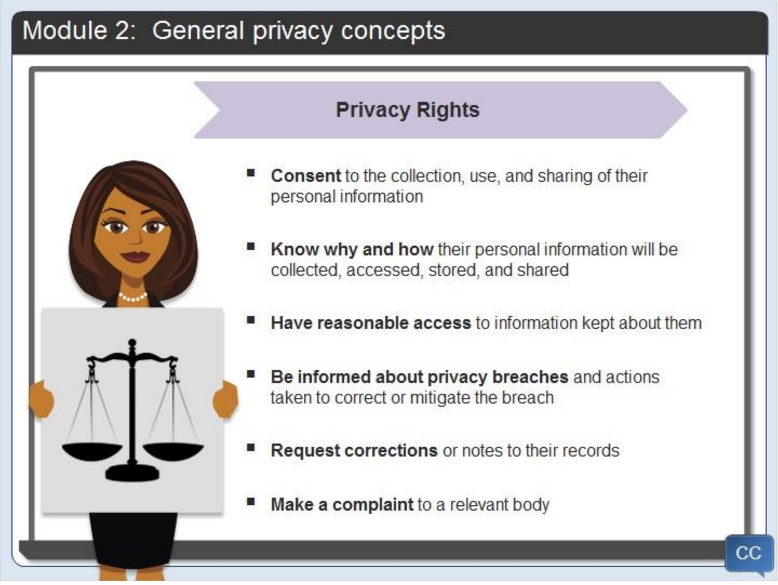
Could you imagine a world where you had no privacy? How would you feel?

Would you be comfortable making certain decisions? Understanding how our information is collected, used, and shared contributes to our ability to be autonomous and feel safe.

You have an important role to play in upholding these rights when you handle sensitive personal information in your daily work.

In module 3, we will expand on what your responsibilities are and explore tips, techniques and resources you can access to make sure you're protecting privacy.

Privacy Rights



Module 2: General privacy concepts

Privacy Rights

- **Consent** to the collection, use, and sharing of their personal information
- **Know why and how** their personal information will be collected, accessed, stored, and shared
- **Have reasonable access** to information kept about them
- **Be informed about privacy breaches** and actions taken to correct or mitigate the breach
- **Request corrections** or notes to their records
- **Make a complaint** to a relevant body

The legislative landscape in Ontario creates general privacy rights for individuals. Individuals have the right to:

Consent to the collection, use, and sharing of their personal information.

Know why and how their personal information will be collected, accessed, stored, and shared.

Have reasonable access to information kept about them.

Be informed about privacy breaches that affect them and the actions taken to correct or mitigate the breach.

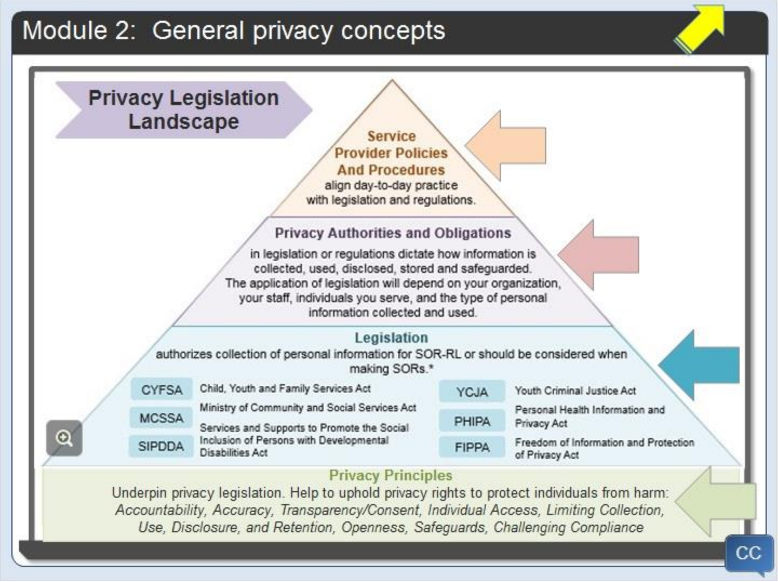
Request corrections or notes to their records.

Make a complaint to a relevant body.

Depending on the legislation that applies in your daily work, there may be some exceptions or considerations for how these rights are applied in SOR-RL.

You should keep privacy rights in mind when you handle personal information.

Privacy Legislation Landscape



Module 2: General privacy concepts

Privacy Legislation Landscape

Service Provider Policies And Procedures align day-to-day practice with legislation and regulations.

Privacy Authorities and Obligations in legislation or regulations dictate how information is collected, used, disclosed, stored and safeguarded. The application of legislation will depend on your organization, your staff, individuals you serve, and the type of personal information collected and used.

Legislation authorizes collection of personal information for SOR-RL or should be considered when making SORs.*

CYFSA	Child, Youth and Family Services Act	YCJA	Youth Criminal Justice Act
MCSSA	Ministry of Community and Social Services Act	PHIPA	Personal Health Information and Privacy Act
SIPDDA	Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act	FIPPA	Freedom of Information and Protection of Privacy Act

Privacy Principles
Underpin privacy legislation. Help to uphold privacy rights to protect individuals from harm:
Accountability, Accuracy, Transparency/Consent, Individual Access, Limiting Collection, Use, Disclosure, and Retention, Openness, Safeguards, Challenging Compliance

This slide provides a visual representation of the privacy legislation landscape. It helps you to think about the landscape like a pyramid where:

The privacy principles listed on the bottom form the foundation and basis for privacy legislation and practice. They are helpful to keep in mind when making decisions about personal information.

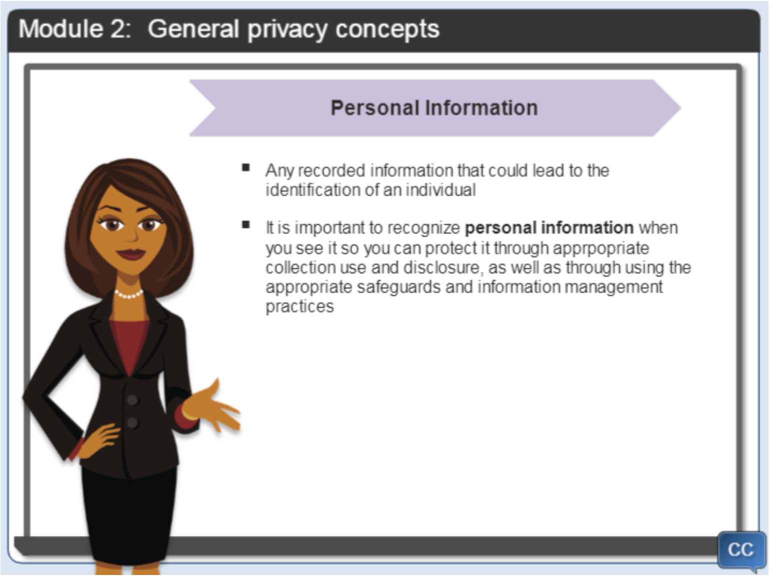
The second tier shows the most common pieces of legislation related to SOR-RL. In Ontario, privacy rights are identified through various pieces of legislation, many of which are specific to the social service sector. In many instances this legislation authorizes the collection of personal information or should be considered when reporting serious occurrences.

those pieces of legislation and their regulations inform when and how that information can be collected, used, disclosed, and retained.

Finally, represented at the top of the pyramid, Service providers should have policies and procedures in place to make sure practice and work reflects legislation and the authorities and obligations.

See the documents in the resources link for more information on the legislative landscape and the privacy principles.

Personal information



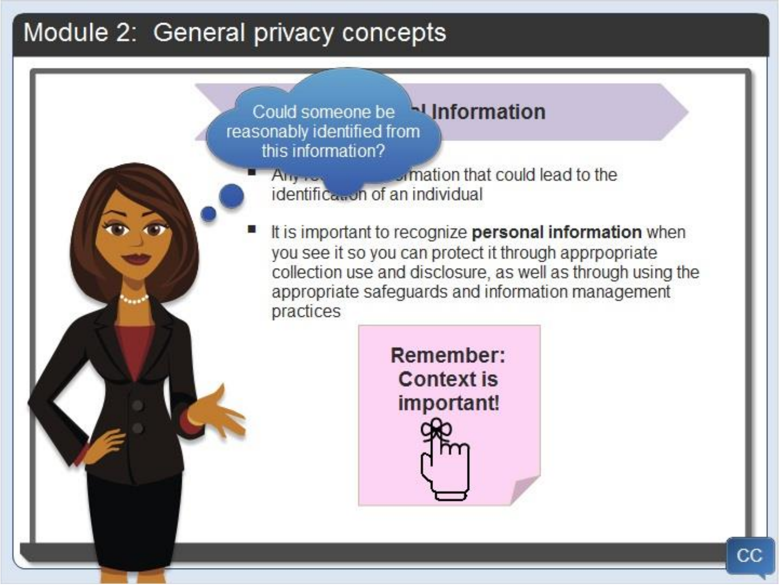
Module 2: General privacy concepts

Personal Information

- Any recorded information that could lead to the identification of an individual
- It is important to recognize **personal information** when you see it so you can protect it through apprpopriate collection use and disclosure, as well as through using the appropriate safeguards and information management practices

In order to protect individuals' privacy rights, it's important that we understand what information may pose a risk to privacy. When entering information into SOR-RL we should treat personal information carefully and with discretion.

Personal information is information that could lead to the identification of an individual. This could include a number of pieces of information, or a single fact.



Module 2: General privacy concepts

Could someone be reasonably identified from this information?

l Information

- Any r rmation that could lead to the identifica n of an individual
- It is important to recognize **personal information** when you see it so you can protect it through apprpopriate collection use and disclosure, as well as through using the appropriate safeguards and information management practices

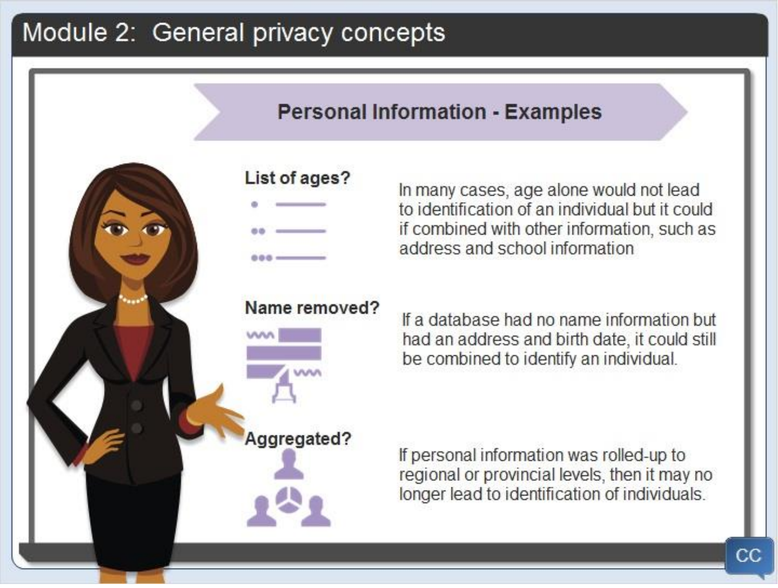
Remember: Context is important!

If you are ever unsure if information is personal information or not, ask yourself this question: Could someone be reasonably identified from this information?

This does not only include if you could identify the individual with the personal information you have, but if others could given their knowledge and background.

For example, if the individual is from a small community, other members of their community may be able to identify them more easily than you with the same piece or pieces of information.

Privacy Rights



Module 2: General privacy concepts

Personal Information - Examples

List of ages?

In many cases, age alone would not lead to identification of an individual but it could if combined with other information, such as address and school information

Name removed?

If a database had no name information but had an address and birth date, it could still be combined to identify an individual.

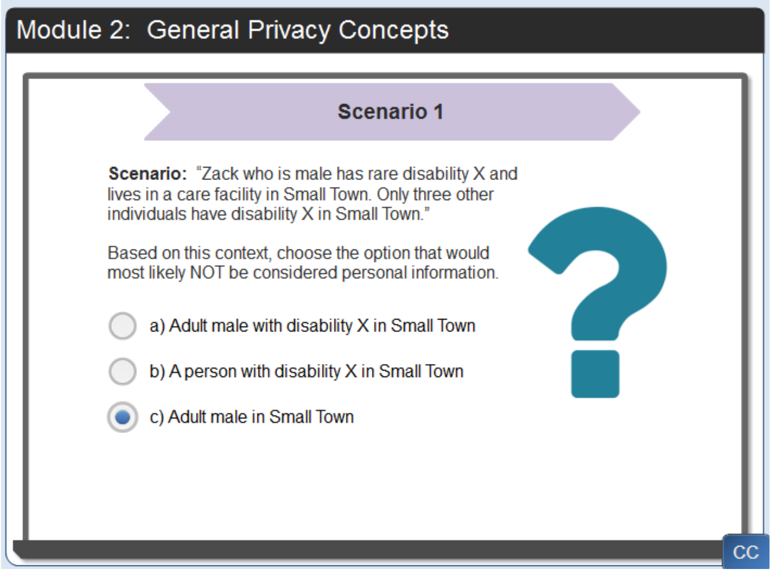
Aggregated?

If personal information was rolled-up to regional or provincial levels, then it may no longer lead to identification of individuals.

Of the examples displayed on the slide, which ones could include personal information? Click on each one to learn more. Click the next button when you are done to continue.

As you might have gathered, the information in these examples could be considered personal information depending on the context. Redacting, or hiding, certain pieces of information such as names, is one way information could be deidentified. However, if other information is available, such as addresses and birth dates, it may not be enough to successfully hide individuals' identities.

Scenario 1



Module 2: General Privacy Concepts

Scenario 1

Scenario: "Zack who is male has rare disability X and lives in a care facility in Small Town. Only three other individuals have disability X in Small Town."

Based on this context, choose the option that would most likely NOT be considered personal information.

○ a) Adult male with disability X in Small Town

○ b) A person with disability X in Small Town

● c) Adult male in Small Town

Read the following scenarios. Based on this context, choose the option that would most likely NOT be considered personal information. Click the submit button to see the answer.

Correct	Choice
	a) Adult male with disability X in Small Town
	b) A person with disability X in Small Town
X	c) Adult male in Small Town

Feedback when incorrect or correct

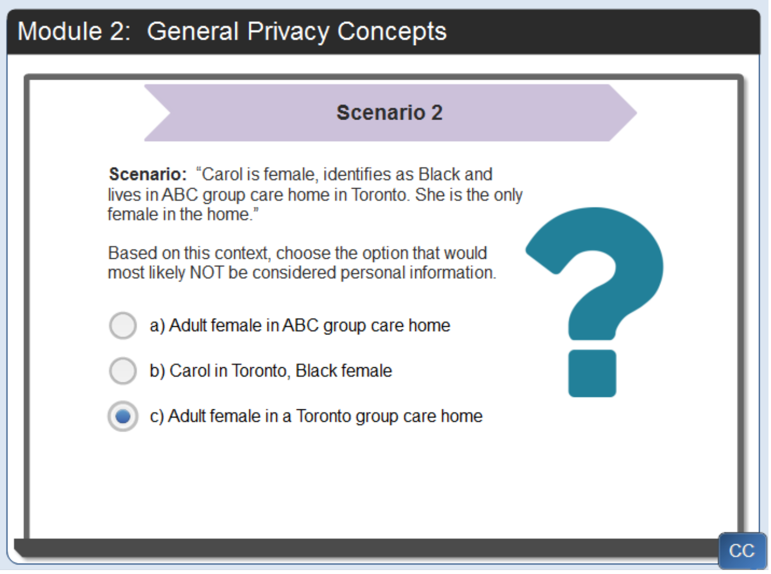
Scenario 1 – Answer Key

a) Adult male with disability X in Small Town - This is personal information. It's reasonable that Zack could be identified with this information since he is one of few people with Disability X in this location.

b) A person with disability X in Small Town - Given that there are so few people in Small Town with disability X, this information may still identify Zack.

c) Adult male in Small Town - CORRECT Based on the information in the scenario, this information is least likely to identify Zack.

Scenario 2


Module 2: General Privacy Concepts

Scenario 2

Scenario: "Carol is female, identifies as Black and lives in ABC group care home in Toronto. She is the only female in the home."

Based on this context, choose the option that would most likely NOT be considered personal information.

○ a) Adult female in ABC group care home

○ b) Carol in Toronto, Black female

● c) Adult female in a Toronto group care home

Read the following scenario. Based on this context, choose the option that would most likely NOT be considered personal information. Click the submit button when you are ready to see the answer. Click the submit button to see the answer.

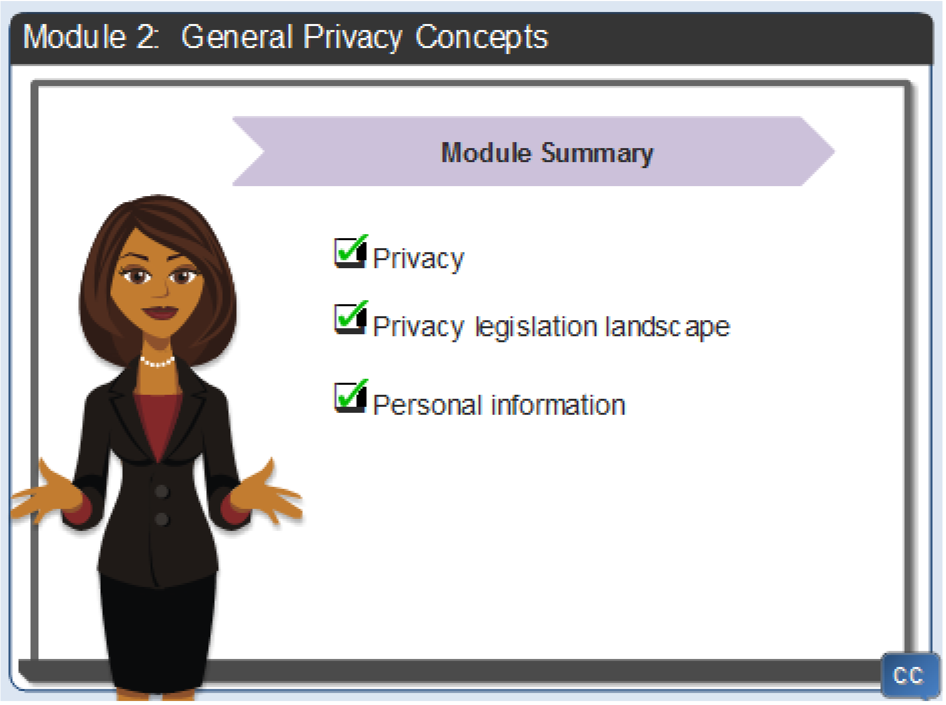
Correct	Choice
	a) Adult female in ABC group care home
	b) Carol in Toronto, Black female

X	c) Adult female in a Toronto group care home

Feedback when correct or incorrect:
Scenario 2 – Answer Key

a) Adult female in ABC group care home - This is personal information. It’s reasonable that someone could identify Carol based on her gender and location, given that she is the only female in her residence.
b) Carol in Toronto, Black female - This would likely be considered personal information since Carol’s first name, location, and ethnicity are used.
c) Adult female in a group care home - CORRECT. Based on what you know from the scenario, this information is least likely to identify Carol.

Module Summary



Module 2: General Privacy Concepts

Module Summary

☑ Privacy

☑ Privacy legislation landscape

☑ Personal information

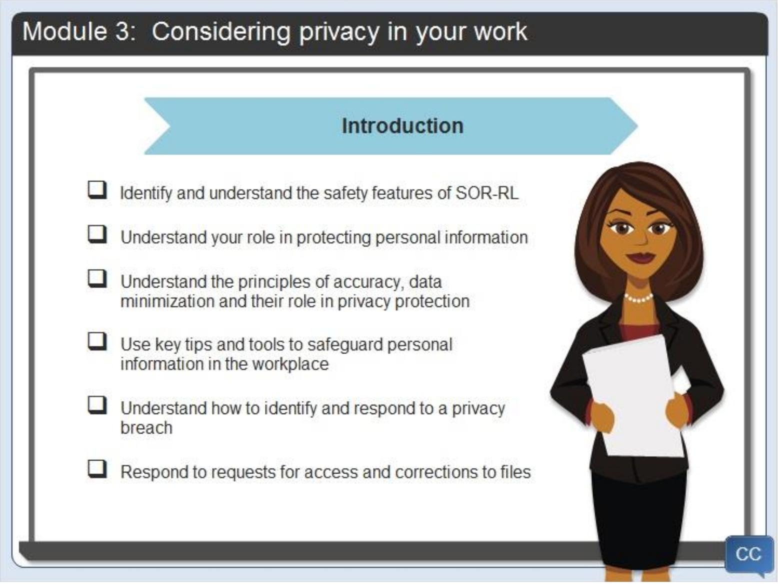
In this module you learned about the different dimensions of privacy and how it's a right.

You learned how to identify and describe the privacy legislative landscape in Ontario.

And, you learned how to define and recognize personal information and why it is important to protect the privacy of personal information.

Module 3: Considering privacy in your work

Introduction



Module 3: Considering privacy in your work

Introduction

- □ Identify and understand the safety features of SOR-RL
- □ Understand your role in protecting personal information
- □ Understand the principles of accuracy, data minimization and their role in privacy protection
- □ Use key tips and tools to safeguard personal information in the workplace
- □ Understand how to identify and respond to a privacy breach
- □ Respond to requests for access and corrections to files

Welcome to module three. In this module we will take a closer look at specific privacy topics and how they relate to your work.

After completing this section, you will be able to:

Identify and understand the safety features of SOR-RL.

Understand your role in protecting personal information.

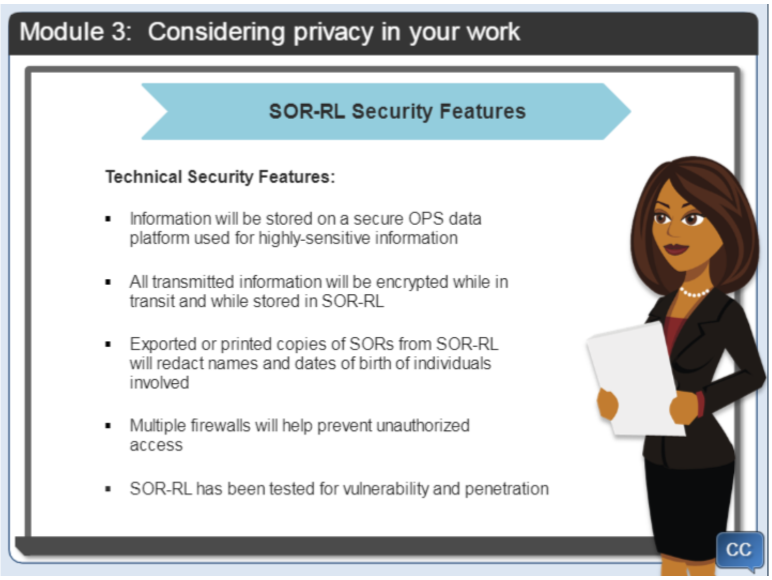
Understand the principles of accuracy, data minimization and their role in privacy protection.

Use key tips and tools to safeguard personal information in the workplace.

Understand how to identify a privacy breach and learn about best practices for responding to a privacy breach.

And how to respond to requests for access and corrections to files.

SOR-RL Security Features



Module 3: Considering privacy in your work

SOR-RL Security Features

Technical Security Features:

- Information will be stored on a secure OPS data platform used for highly-sensitive information
- All transmitted information will be encrypted while in transit and while stored in SOR-RL
- Exported or printed copies of SORs from SOR-RL will redact names and dates of birth of individuals involved
- Multiple firewalls will help prevent unauthorized access
- SOR-RL has been tested for vulnerability and penetration

The Ministry of Children, Community and Social Services is improving processes for serious occurrence reporting and children's residential licensing to support better outcomes for some of Ontario's most vulnerable children, youth and adults. This includes the creation of SOR-RL to replace the manual processes for serious occurrence reporting to make reporting easier and more secure.

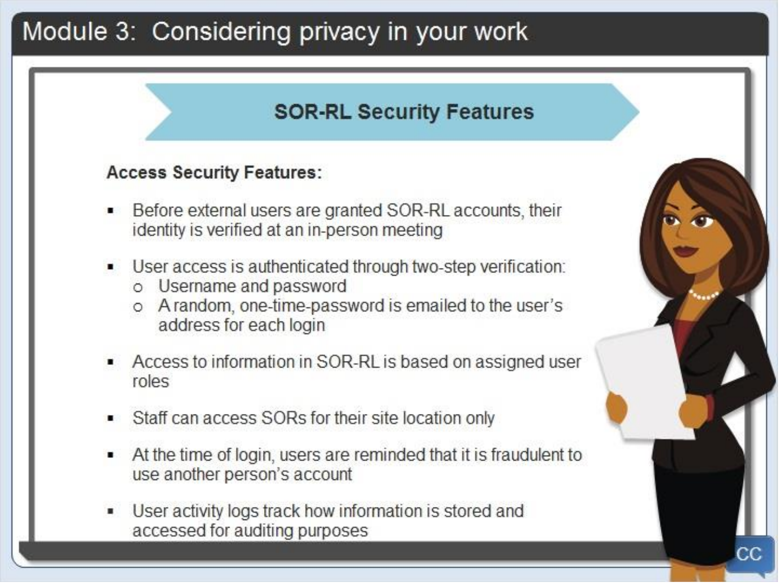
MCCSS understands the importance of keeping the sensitive information that will be entered into SOR-RL secure. For this reason, SOR-RL has built-in security features to support the safeguarding of information:

I'll start by listing the technical security features.

Information will be stored on a secure O P S data platform used for highly-sensitive information.

All transmitted information will be encrypted while in transit and while stored in SOR-RL.
Exported or printed copies of SORs from SOR-RL will redact names and dates of birth of individuals involved.
Multiple firewalls will help prevent unauthorized access.
SOR-RL has been tested for vulnerability and penetration.

SOR-RL Security Features



Module 3: Considering privacy in your work

SOR-RL Security Features

Access Security Features:

- Before external users are granted SOR-RL accounts, their identity is verified at an in-person meeting
- User access is authenticated through two-step verification:
  - Username and password
  - A random, one-time-password is emailed to the user's address for each login
- Access to information in SOR-RL is based on assigned user roles
- Staff can access SORs for their site location only
- At the time of login, users are reminded that it is fraudulent to use another person's account
- User activity logs track how information is stored and accessed for auditing purposes

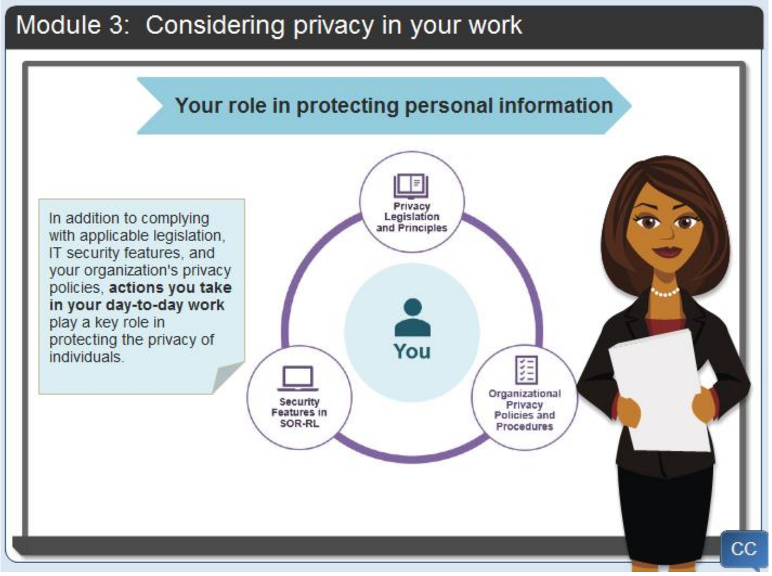
There is also security built into the access features of SOR-RL.

Before external users are granted SOR-RL accounts, their identity is verified at an in-person meeting.
User access is authenticated through two-step verification including Username and password and a random, one-time-password which will be emailed to the user's address for each login.
Access to information in SOR-RL is based on assigned user roles.
Staff can access SORs for their site location only.

At the time of login, users are reminded that it is fraudulent to use another person's account.

And lastly, user activity logs track how information is stored and accessed for auditing purposes.

Your role in protecting personal information



Module 3: Considering privacy in your work

Your role in protecting personal information

In addition to complying with applicable legislation, IT security features, and your organization's privacy policies, **actions you take in your day-to-day work** play a key role in protecting the privacy of individuals.

Privacy Legislation and Principles

You

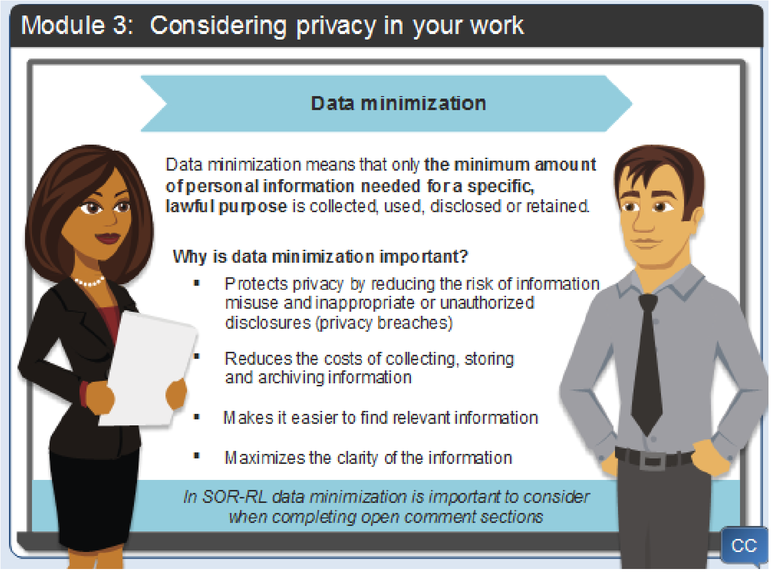
Security Features in SOR-RL

Organizational Privacy Policies and Procedures

In addition to complying with applicable legislation, IT security features, and your organization's privacy policies, actions you take in your day to day work play a key role in protecting the privacy of individuals.

We will talk more about your role as we explore data minimization, preventing privacy breaches, fulfilling access requests and more.

Data minimization



Module 3: Considering privacy in your work

Data minimization

Data minimization means that only **the minimum amount of personal information needed for a specific, lawful purpose** is collected, used, disclosed or retained.

Why is data minimization important?

- Protects privacy by reducing the risk of information misuse and inappropriate or unauthorized disclosures (privacy breaches)
- Reduces the costs of collecting, storing and archiving information
- Makes it easier to find relevant information
- Maximizes the clarity of the information

In SOR-RL data minimization is important to consider when completing open comment sections

The first concept we'll cover is Data Minimization.

Robert: What is that Lisa?

Lisa: Data minimization means that only the minimum amount of personal information needed for the specific purpose is collected, used, disclosed or retained. Data minimization was an important consideration in the creation of SOR-RL.

Remembering the purpose for making serious occurrence reports will also help you to determine which personal information, if any, is appropriate to include in the open comment sections. To review, the main purpose of serious occurrence reporting is to monitor serious occurrences when they happen, prevent future serious occurrences, and to allow the ministry to fulfill their oversight role.

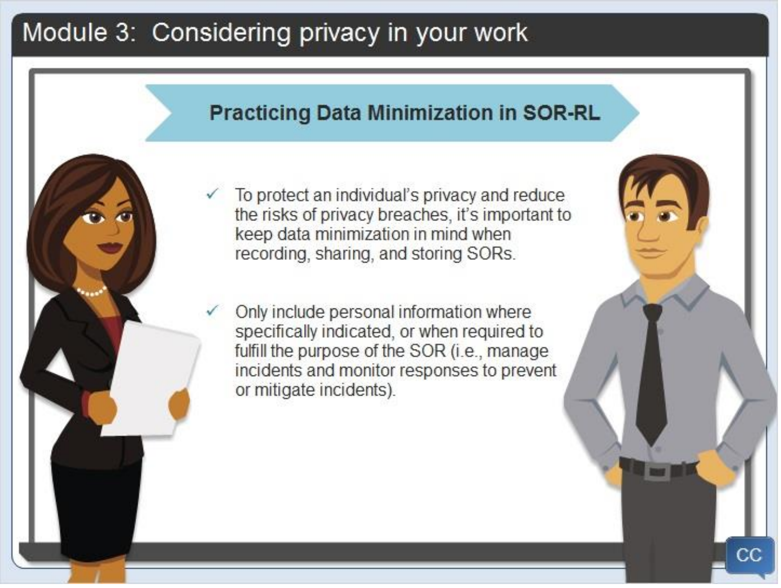
Robert: Why is data minimization important?

Lisa: It protects privacy by reducing the risk of data misuse and inappropriate disclosures.

It reduces the costs of collecting, storing and archiving data.

And data minimization makes it easier to find relevant information and maximizes the clarity of the information.

Practicing Data Minimization in SOR-RL



Module 3: Considering privacy in your work

Practicing Data Minimization in SOR-RL

- ✓ To protect an individual's privacy and reduce the risks of privacy breaches, it's important to keep data minimization in mind when recording, sharing, and storing SORs.
- ✓ Only include personal information where specifically indicated, or when required to fulfill the purpose of the SOR (i.e., manage incidents and monitor responses to prevent or mitigate incidents).

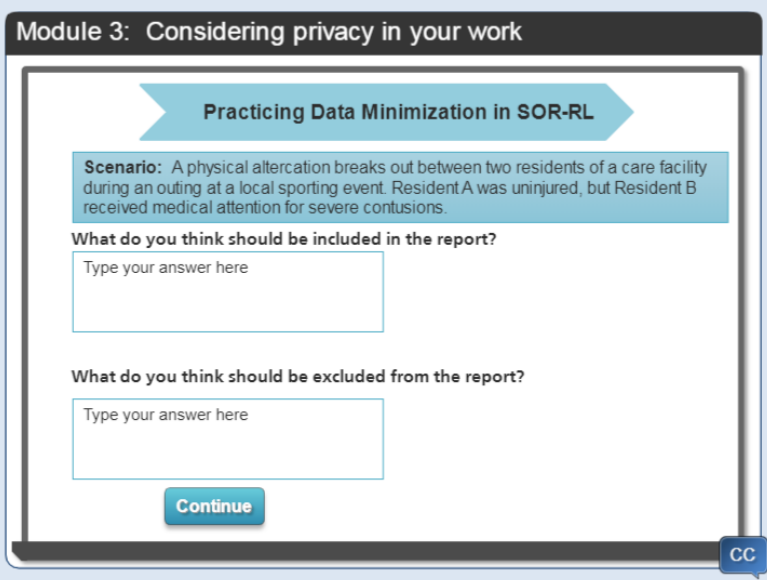
It's important to keep data minimization in mind when recording, sharing and storing SORs.

When completing open comment sections in SOR-RL, only include personal information where specifically indicated, or when required to fulfill the purpose.

Robert: Lisa, can you give me an example on how data minimization could be used in my work?

Lisa: Certainly, I have a scenario for you to think about on the next slide to test your understanding.

Practicing Data Minimization in SOR-RL



Module 3: Considering privacy in your work

Practicing Data Minimization in SOR-RL

Scenario: A physical altercation breaks out between two residents of a care facility during an outing at a local sporting event. Resident A was uninjured, but Resident B received medical attention for severe contusions.

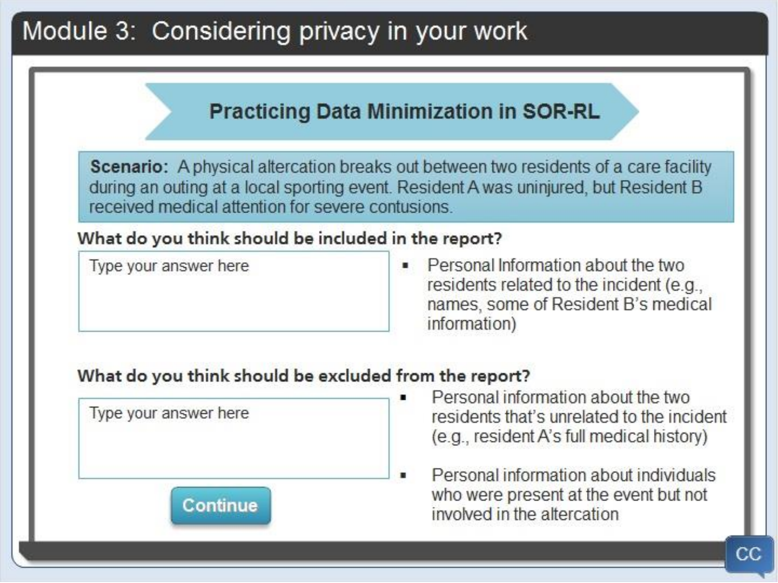
What do you think should be included in the report?

Type your answer here

What do you think should be excluded from the report?

Type your answer here

Take a minute to read the scenario and answer the questions. Click continue when you are done.



Module 3: Considering privacy in your work

Practicing Data Minimization in SOR-RL

Scenario: A physical altercation breaks out between two residents of a care facility during an outing at a local sporting event. Resident A was uninjured, but Resident B received medical attention for severe contusions.

What do you think should be included in the report?

Type your answer here

- Personal Information about the two residents related to the incident (e.g., names, some of Resident B's medical information)

What do you think should be excluded from the report?

Type your answer here

- Personal information about the two residents that's unrelated to the incident (e.g., resident A's full medical history)
- Personal information about individuals who were present at the event but not involved in the altercation

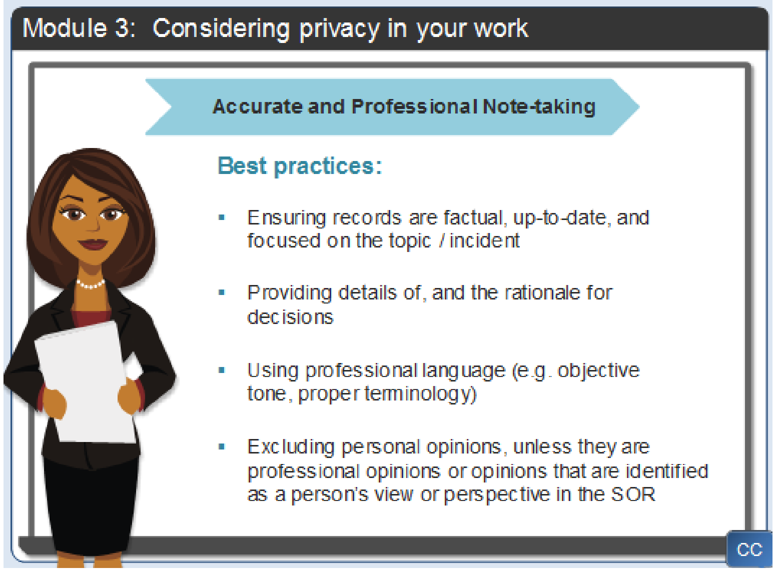
You should only include information that is reasonably necessary to respond to and monitor the incident, or prevent future incidents and exclude personal information that is unnecessary to those purposes.

For example, since Resident A was uninjured, their medical history is not likely to be pertinent to the SOR, unless it's helpful for context on why the altercation happened, how it could be resolved, or how future altercations could be prevented. Limited information about medical history may be requested by a ministry staff only if needed to better understand the serious occurrence and / or to better support the development of a responsive action plan.

When responding to similar incidents, you'll need to use your judgment and knowledge of the specific details of the incident to include the appropriate information.

You should refer to the MCCSS SOR Guidelines, 2019 for details on what specific information needs to be included in the SOR description, depending on the category of the serious occurrence.

Accurate and Professional Note-taking



Module 3: Considering privacy in your work

Accurate and Professional Note-taking

Best practices:

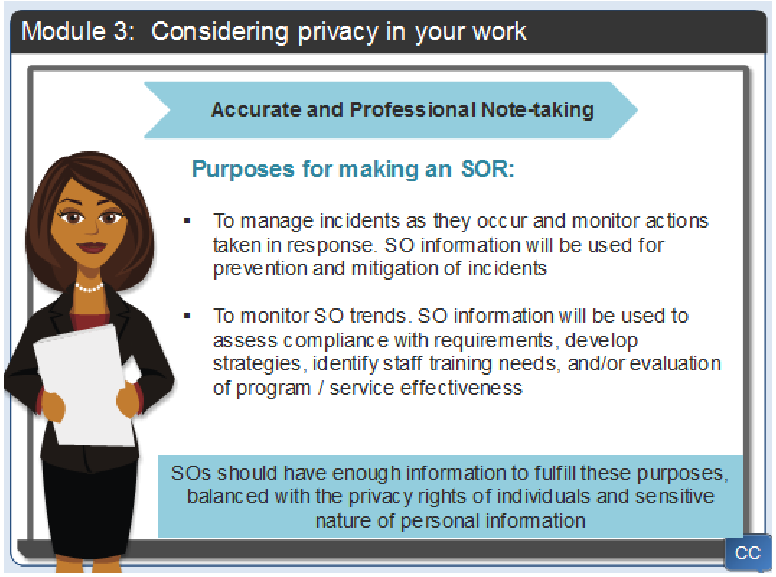
- Ensuring records are factual, up-to-date, and focused on the topic / incident
- Providing details of, and the rationale for decisions
- Using professional language (e.g. objective tone, proper terminology)
- Excluding personal opinions, unless they are professional opinions or opinions that are identified as a person's view or perspective in the SOR

It is important to keep in mind both your purpose for reporting a serious occurrence and that individuals have a right to access their information.

As such, you should make efforts to ensure that personal information included in serious occurrence reports is kept at a minimal, accurate and professional.

Best practices include:
Ensuring records are factual, up-to-date, and focused on the topic or incident.
Providing details of and the rationale for decisions.
Using professional language (e.g., objective tone, proper terminology).
Excluding personal opinions, unless they are professional opinions or opinions that are identified as a person's view or perspective in the SOR.

Accurate and Professional Note-taking



Module 3: Considering privacy in your work

Accurate and Professional Note-taking

Purposes for making an SOR:

- To manage incidents as they occur and monitor actions taken in response. SO information will be used for prevention and mitigation of incidents
- To monitor SO trends. SO information will be used to assess compliance with requirements, develop strategies, identify staff training needs, and/or evaluation of program / service effectiveness

SOs should have enough information to fulfill these purposes, balanced with the privacy rights of individuals and sensitive nature of personal information

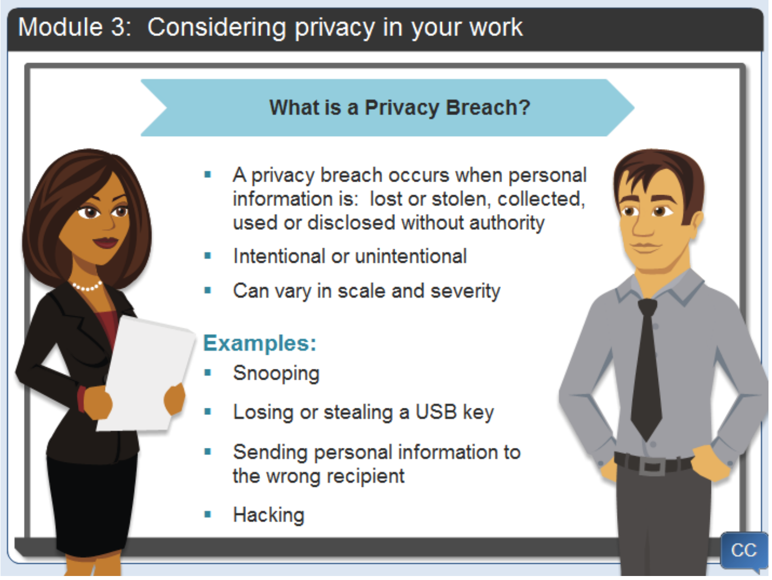
As a refresher, let’s review the purposes for SORs.

SORs are used to manage incidents as they occur and monitor responses to the incident. Serious occurrence information will be used for prevention or mitigation of incidents.

SORs will also support MCCSS in monitoring and overseeing service providers in the delivery of services.

Serious occurrence reports should have enough information to fulfill these purposes, balanced with the privacy rights of individuals and sensitive nature of personal information.

What is a Privacy Breach?



Module 3: Considering privacy in your work

What is a Privacy Breach?

- A privacy breach occurs when personal information is: lost or stolen, collected, used or disclosed without authority
- Intentional or unintentional
- Can vary in scale and severity

Examples:

- Snooping
- Losing or stealing a USB key
- Sending personal information to the wrong recipient
- Hacking

Robert: Lisa, what is a privacy breach, and can you give me a few examples?

Lisa: A privacy breach is when personal information is lost or stolen; or collected, used, or disclosed without authority.

A privacy breach may be intentional or unintentional and can vary in scale and severity.

Examples of privacy breaches include:

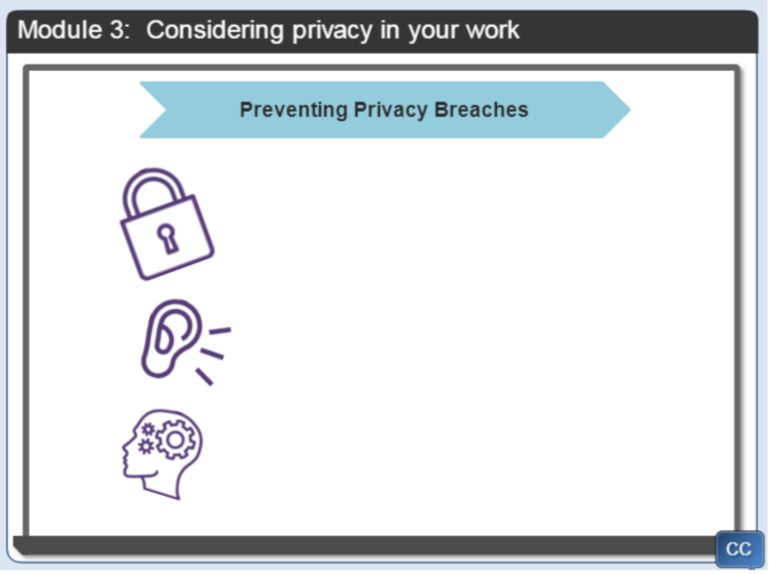
'Snooping' or accessing files containing personal information when not necessary or without authority.

Losing or stealing a USB key with personal information on it.

Emailing files with personal information to someone who doesn't have the authority to see them, or having a conversation involving personal information where others may overhear.

Hacking an electronic database containing personal information such as a ransomware attack.

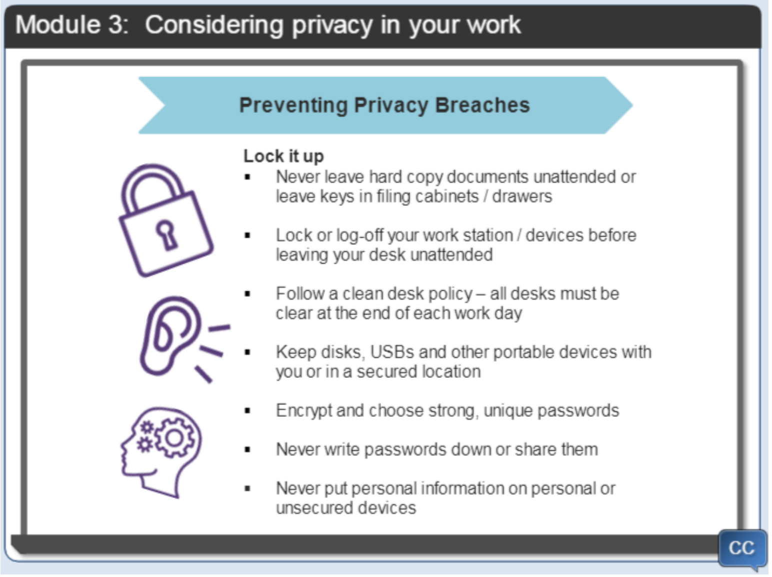
Preventing Privacy Breaches


Module 3: Considering privacy in your work
Preventing Privacy Breaches
CC

We're all faced with many choices throughout the day. Regularly checking in with yourself to make sure you're following policies, procedures, and keeping in mind privacy principles is one of the ways to prevent privacy breaches.

Securing personal information and protecting privacy starts with you as a service provider.

Click on each symbol to learn some tips to help you ensure information isn't lost, stolen, disclosed or used without permission.

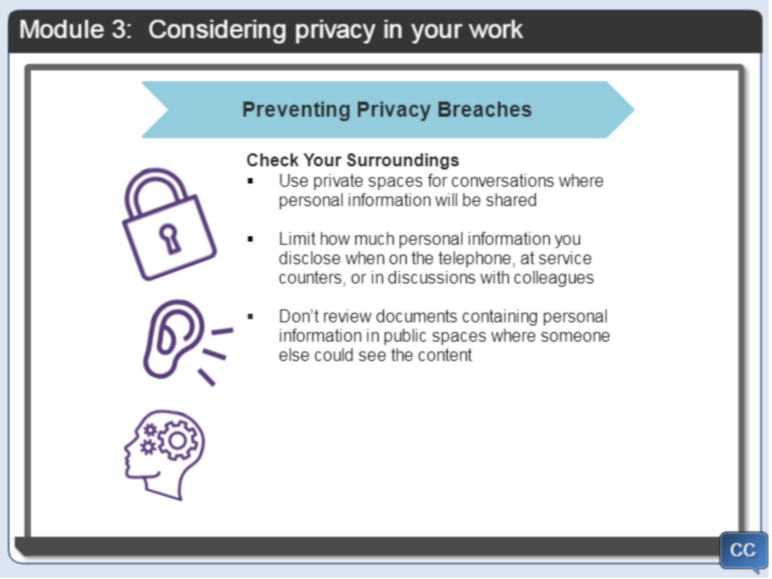


Module 3: Considering privacy in your work

Preventing Privacy Breaches

Lock it up

- Never leave hard copy documents unattended or leave keys in filing cabinets / drawers
- Lock or log-off your work station / devices before leaving your desk unattended
- Follow a clean desk policy – all desks must be clear at the end of each work day
- Keep disks, USBs and other portable devices with you or in a secured location
- Encrypt and choose strong, unique passwords
- Never write passwords down or share them
- Never put personal information on personal or unsecured devices

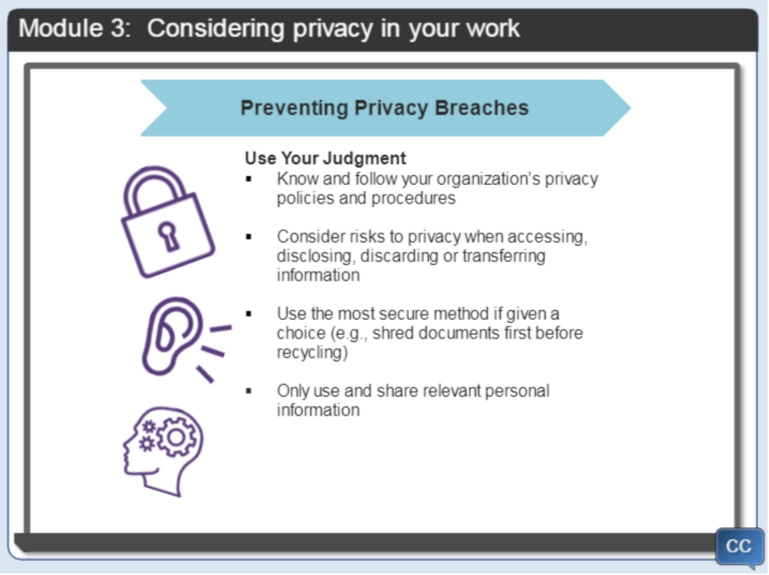


Module 3: Considering privacy in your work

Preventing Privacy Breaches

Check Your Surroundings

- Use private spaces for conversations where personal information will be shared
- Limit how much personal information you disclose when on the telephone, at service counters, or in discussions with colleagues
- Don't review documents containing personal information in public spaces where someone else could see the content



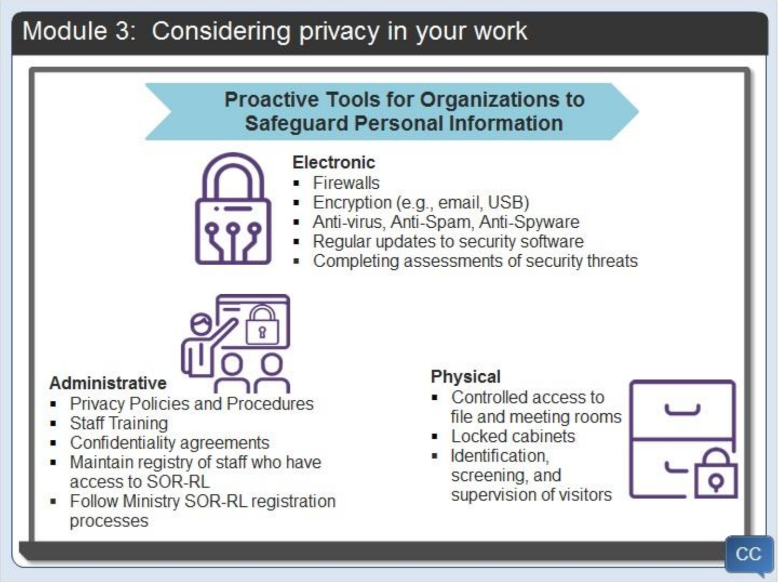
Module 3: Considering privacy in your work

Preventing Privacy Breaches

Use Your Judgment

- Know and follow your organization's privacy policies and procedures
- Consider risks to privacy when accessing, disclosing, discarding or transferring information
- Use the most secure method if given a choice (e.g., shred documents first before recycling)
- Only use and share relevant personal information

Proactive Tools



Module 3: Considering privacy in your work

Proactive Tools for Organizations to Safeguard Personal Information

Electronic

- Firewalls
- Encryption (e.g., email, USB)
- Anti-virus, Anti-Spam, Anti-Spyware
- Regular updates to security software
- Completing assessments of security threats

Administrative

- Privacy Policies and Procedures
- Staff Training
- Confidentiality agreements
- Maintain registry of staff who have access to SOR-RL
- Follow Ministry SOR-RL registration processes

Physical

- Controlled access to file and meeting rooms
- Locked cabinets
- Identification, screening, and supervision of visitors

In addition to the actions you can take as an individual to protect privacy, your organization can put several measures in place to support you.

For example: Electronic supports for your work computer and smartphone like firewalls, regular updates to security software, and data encryption, such as encrypted USB keys.

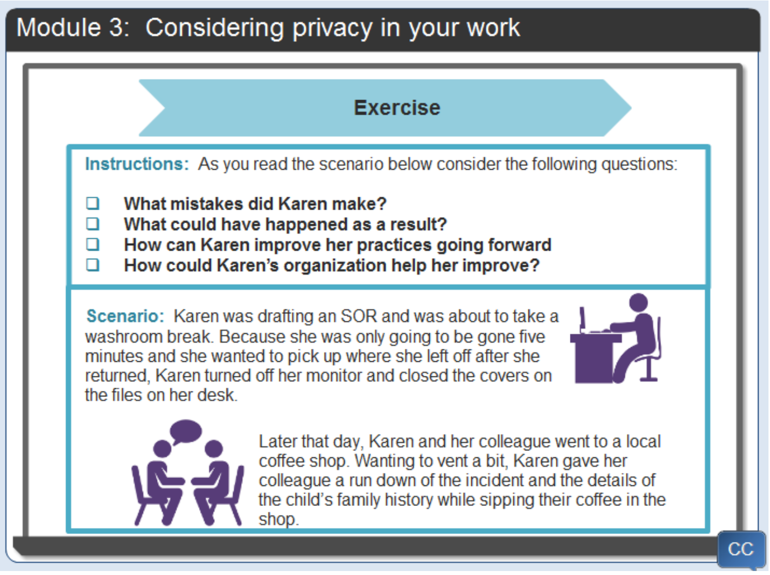
Training on their privacy policies and procedures.

Key card access to secure rooms, locking filing cabinets and procedures for secure file disposal or transfer.

For SOR-RL specifically, organizations should have a registry of staff who have access to the system and they should follow the registration process set out by the ministry.

Your organization may also want to put in place measures to ensure rules are followed and procedures are in place when issues do occur.

Exercise



Module 3: Considering privacy in your work

Exercise

Instructions: As you read the scenario below consider the following questions:

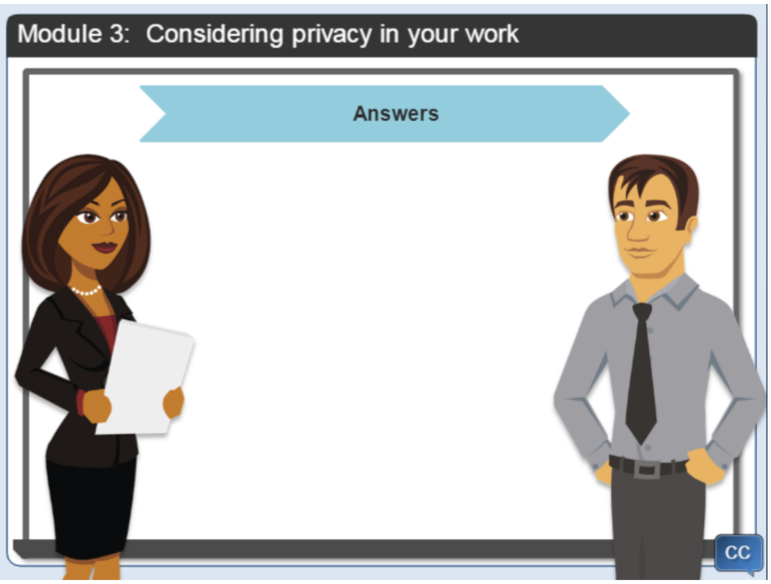
- ❑ **What mistakes did Karen make?**
- ❑ **What could have happened as a result?**
- ❑ **How can Karen improve her practices going forward**
- ❑ **How could Karen's organization help her improve?**

Scenario: Karen was drafting an SOR and was about to take a washroom break. Because she was only going to be gone five minutes and she wanted to pick up where she left off after she returned, Karen turned off her monitor and closed the covers on the files on her desk.

Later that day, Karen and her colleague went to a local coffee shop. Wanting to vent a bit, Karen gave her colleague a run down of the incident and the details of the child's family history while sipping their coffee in the shop.

As you read the scenario consider the questions listed at the top of the slide. You may want to jot down your answers on paper. We'll review the answers on the next slide.

Answers

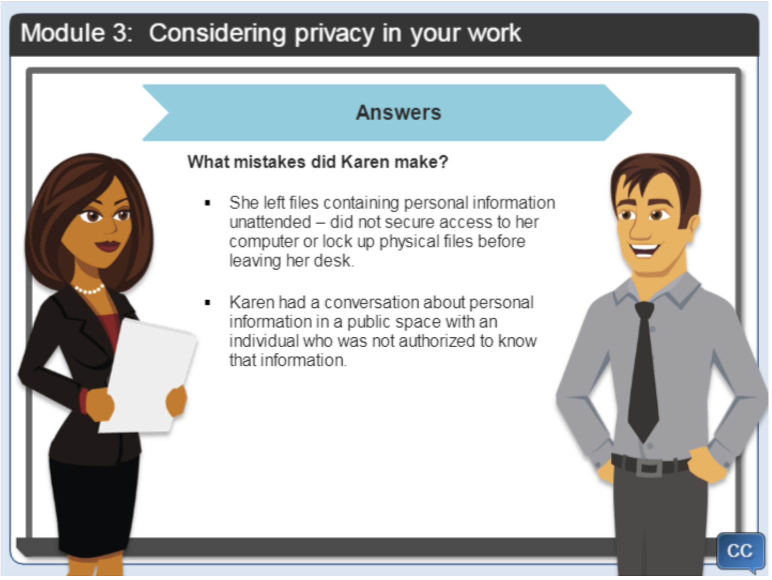


Module 3: Considering privacy in your work

Answers

Lisa: Robert, are you ready to compare your answers.

Robert: Sure. Some mistakes were pretty obvious.



Module 3: Considering privacy in your work

Answers

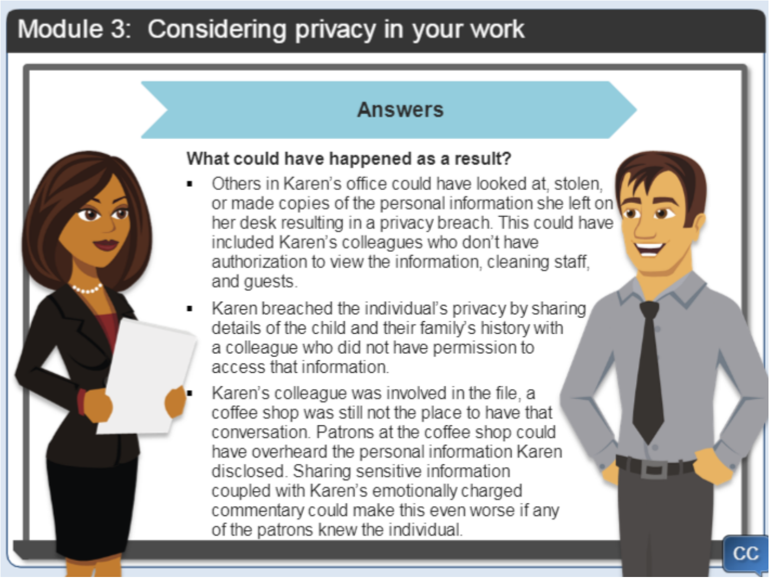
What mistakes did Karen make?

- She left files containing personal information unattended – did not secure access to her computer or lock up physical files before leaving her desk.
- Karen had a conversation about personal information in a public space with an individual who was not authorized to know that information.

Lisa: What mistakes did Karen make?

Robert: She left files containing personal information unattended - did not secure access to her computer or lock up physical files before leaving her desk.

Karen had a conversation about personal information in a public space with an individual who was not authorized to know that information.



Module 3: Considering privacy in your work

Answers

What could have happened as a result?

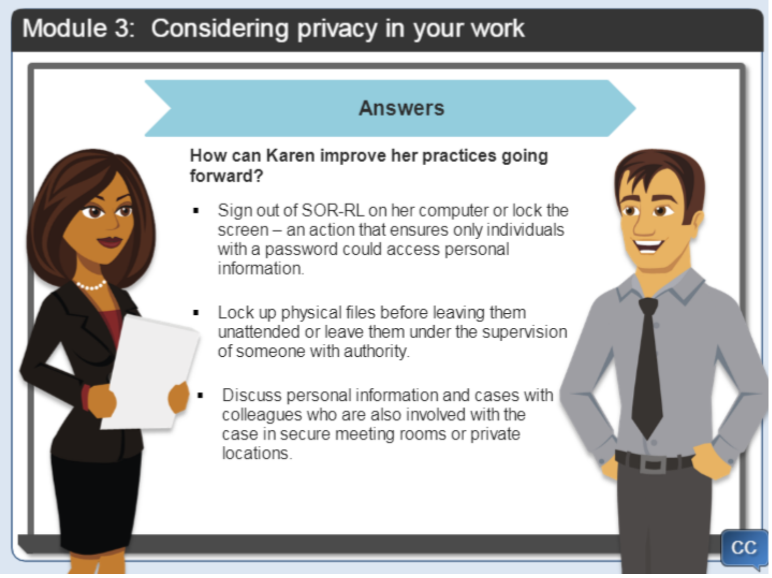
- Others in Karen's office could have looked at, stolen, or made copies of the personal information she left on her desk resulting in a privacy breach. This could have included Karen's colleagues who don't have authorization to view the information, cleaning staff, and guests.
- Karen breached the individual's privacy by sharing details of the child and their family's history with a colleague who did not have permission to access that information.
- Karen's colleague was involved in the file, a coffee shop was still not the place to have that conversation. Patrons at the coffee shop could have overheard the personal information Karen disclosed. Sharing sensitive information coupled with Karen's emotionally charged commentary could make this even worse if any of the patrons knew the individual.

Lisa: What happened or could have happened as a result?

Robert: Others in Karen's office could have looked at, stolen, or made copies (e.g., taken pictures of documents with their phone) of the personal information she left on her desk resulting in a privacy breach. This could have included Karen's colleagues who don't have authorization to view the information, cleaning staff, and guests.

Karen breached the individual's privacy by sharing details of the child and their family's history with a colleague who did not have permission to access that information.

If Karen's colleague was involved in the file, a coffee shop was still not the place to have that conversation. Patrons at the coffee shop could have overheard the personal information Karen disclosed. Sharing sensitive information coupled with Karen's emotionally charged commentary could make this even worse if any of the patrons knew the individual.



Module 3: Considering privacy in your work

Answers

How can Karen improve her practices going forward?

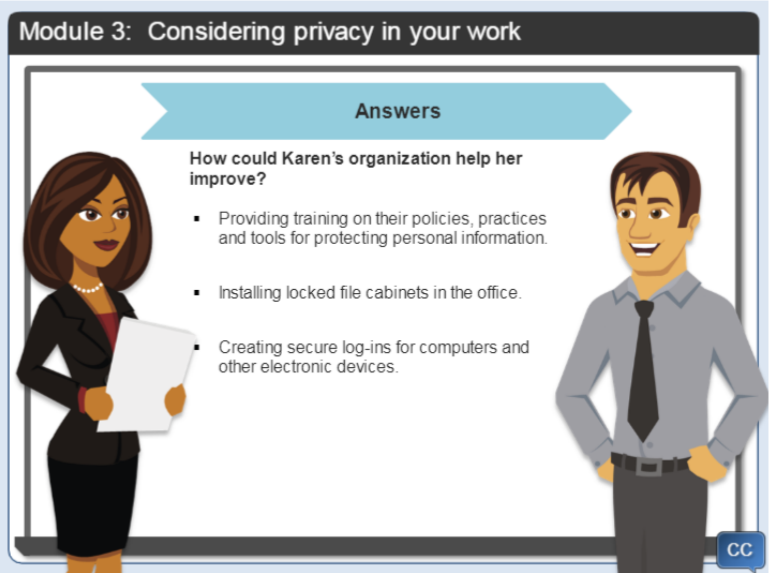
- Sign out of SOR-RL on her computer or lock the screen – an action that ensures only individuals with a password could access personal information.
- Lock up physical files before leaving them unattended or leave them under the supervision of someone with authority.
- Discuss personal information and cases with colleagues who are also involved with the case in secure meeting rooms or private locations.

Lisa: How can Karen improve her practices going forward?

Robert: Sign out of SOR-RL on her computer or lock the screen - an action that ensures only individuals with a password could access personal information.

Lock up physical files before leaving them unattended or leave them under the supervision of someone with authority.

Discuss personal information and cases with colleagues who are also involved with the case in secure meeting rooms or private locations.



Module 3: Considering privacy in your work

Answers

How could Karen's organization help her improve?

- Providing training on their policies, practices and tools for protecting personal information.
- Installing locked file cabinets in the office.
- Creating secure log-ins for computers and other electronic devices.

Lisa: How could Karen's organization help her improve?

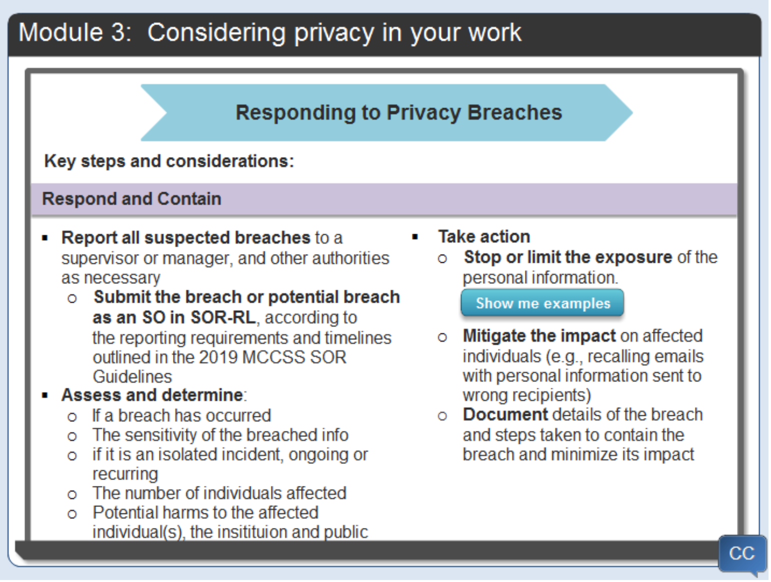
Robert: Providing training on their policies, practices and tools for protecting personal information.

Installing locked file cabinets in the office.

Creating secure log-ins for computers and other electronic devices.

Lisa: That was pretty good Robert. Let's go on and see what we should do if a breach occurs.

Responding to Privacy Breaches



Module 3: Considering privacy in your work

Responding to Privacy Breaches

Key steps and considerations:

Respond and Contain

- **Report all suspected breaches** to a supervisor or manager, and other authorities as necessary
  - **Submit the breach or potential breach as an SO in SOR-RL**, according to the reporting requirements and timelines outlined in the 2019 MCCSS SOR Guidelines
- **Assess and determine**:
  - If a breach has occurred
  - The sensitivity of the breached info
  - if it is an isolated incident, ongoing or recurring
  - The number of individuals affected
  - Potential harms to the affected individual(s), the insitituion and public
- **Take action**
  - **Stop or limit the exposure** of the personal information.

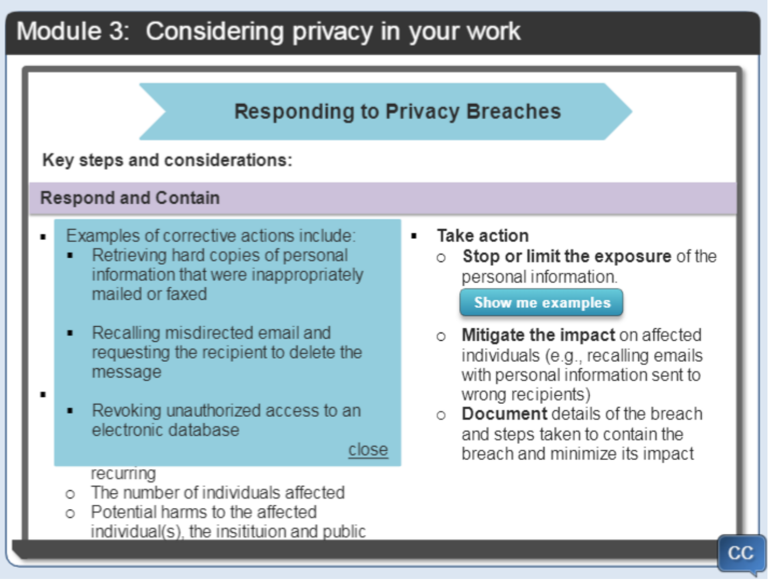
    Show me examples
  - **Mitigate the impact** on affected individuals (e.g., recalling emails with personal information sent to wrong recipients)
  - **Document** details of the breach and steps taken to contain the breach and minimize its impact

Despite best efforts, privacy breaches may still occur. Organizations should establish protocols for responding to privacy breaches. Here are some key steps and considerations that should be used to inform privacy breach responses.

Respond and Contain:
Report all suspected breaches to a supervisor or manager, and other authorities as necessary.
Submit the breach or potential breach as a serious occurrence in SOR-RL, according to the reporting requirements and timelines outlined in the 2019 MCCSS SOR Guidelines.

Assess and determine:
If a breach has occurred.
The sensitivity of the breached information.
If it is an isolated incident, ongoing or recurring.
The number of individuals affected.
Potential harms to affected individuals, the institution and public.

Take Action:
Stop or limit the exposure of the personal information.
Mitigate the impact on affected individuals (e.g., recalling emails with personal information sent to wrong recipients).
Document details of the breach and steps taken to contain the breach and minimize its impact.



Module 3: Considering privacy in your work

Responding to Privacy Breaches

Key steps and considerations:

Respond and Contain

- Examples of corrective actions include:
  - Retrieving hard copies of personal information that were inappropriately mailed or faxed
  - Recalling misdirected email and requesting the recipient to delete the message
  - Revoking unauthorized access to an electronic database

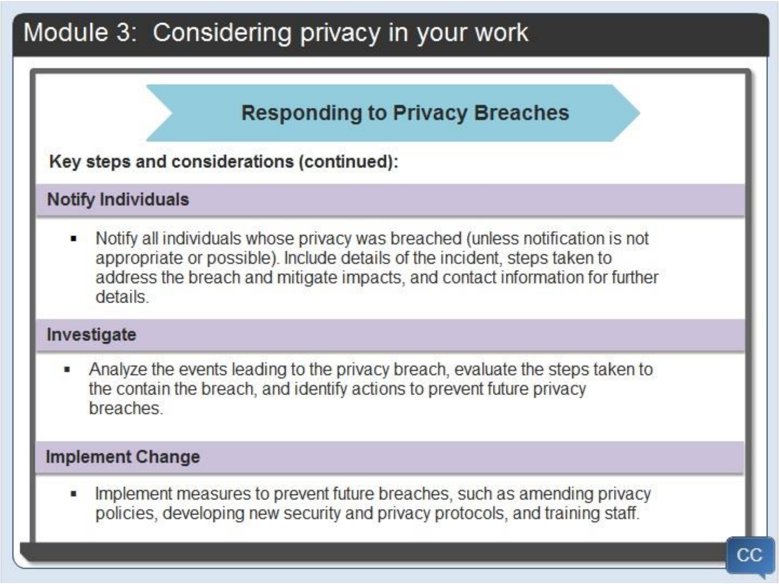
  close

  recurring
  - The number of individuals affected
  - Potential harms to the affected individual(s), the insitituion and public

- **Take action**
  - **Stop or limit the exposure** of the personal information.

  - **Mitigate the impact** on affected individuals (e.g., recalling emails with personal information sent to wrong recipients)
  - **Document** details of the breach and steps taken to contain the breach and minimize its impact

Responding to Privacy Breaches



Module 3: Considering privacy in your work

Responding to Privacy Breaches

Key steps and considerations (continued):

Notify Individuals

- Notify all individuals whose privacy was breached (unless notification is not appropriate or possible). Include details of the incident, steps taken to address the breach and mitigate impacts, and contact information for further details.

Investigate

- Analyze the events leading to the privacy breach, evaluate the steps taken to the contain the breach, and identify actions to prevent future privacy breaches.

Implement Change

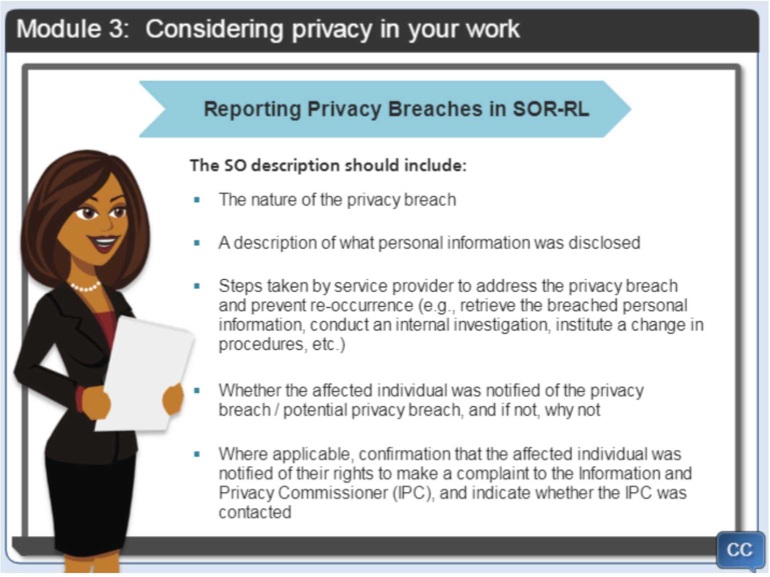
- Implement measures to prevent future breaches, such as amending privacy policies, developing new security and privacy protocols, and training staff.

Notify all individuals whose privacy was breached (unless notification is not appropriate or possible). Include details of the incident, steps taken to address the breach and mitigate impacts, and contact information for further details.

Investigate. Analyze the events leading to the privacy breach, evaluate the steps taken to contain the breach, and identify actions to prevent future breaches.

Lastly, implement measures to prevent future breaches, such as amending privacy policies, developing new security and privacy protocols, and training staff.

Responding to Privacy Breaches



Module 3: Considering privacy in your work

Reporting Privacy Breaches in SOR-RL

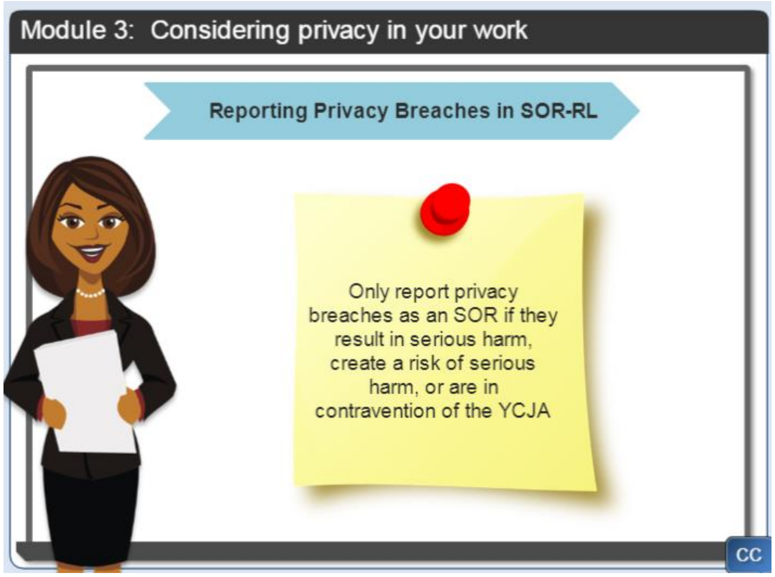
The SO description should include:

- The nature of the privacy breach
- A description of what personal information was disclosed
- Steps taken by service provider to address the privacy breach and prevent re-occurrence (e.g., retrieve the breached personal information, conduct an internal investigation, institute a change in procedures, etc.)
- Whether the affected individual was notified of the privacy breach / potential privacy breach, and if not, why not
- Where applicable, confirmation that the affected individual was notified of their rights to make a complaint to the Information and Privacy Commissioner (IPC), and indicate whether the IPC was contacted

If there is a privacy breach or a potential breach of privacy that results in serious harm or risk of serious harm to the individual and / or others, or is in contravention of the Youth Criminal Justice Act (YCJA), it must be reported as an SOR.

All privacy breaches that meet this criteria are considered to be a Level 1 SOR, which requires service providers to immediately notify the ministry and submit an SOR within 1 hour of becoming aware of the serious occurrence or deeming the incident to be a serious occurrence.

The SO description should include:
The nature of the privacy breach.
Description of what personal information was disclosed.
Steps taken by service provider to address the privacy breach and prevent re-occurrence (e.g., retrieve the breached personal information, conduct an internal investigation, institute a change in procedures, etc.).
Whether the affected individual was notified of the privacy breach / potential privacy breach, and if not, why not.
Where applicable, confirmation that the affected individual was notified of their rights to make a complaint to the Information and Privacy Commissioner (IPC), and indicate whether the IPC was contacted.

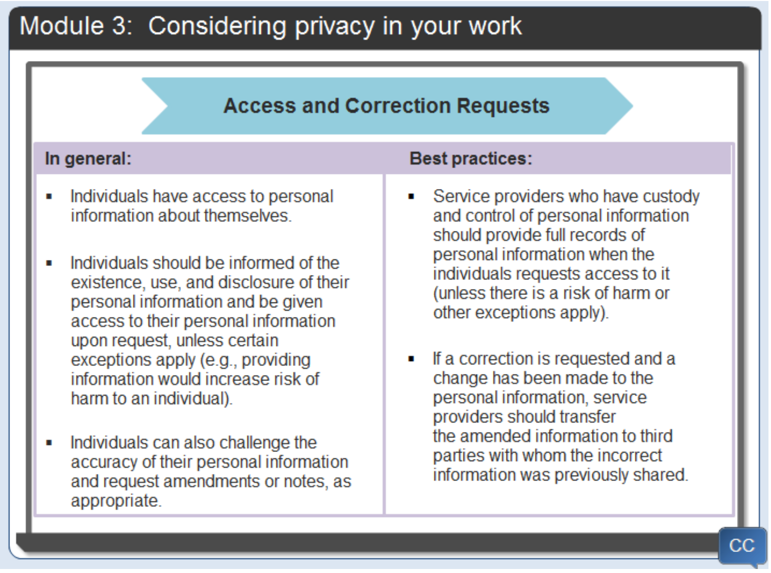

Module 3: Considering privacy in your work

Reporting Privacy Breaches in SOR-RL

Only report privacy breaches as an SOR if they result in serious harm, create a risk of serious harm, or are in contravention of the YCJA

It is very important to remember to only report privacy breaches as an SOR if they result in serious harm, create a risk of serious harm, or are in contravention of the YCJA.

Access and Correction Requests



Module 3: Considering privacy in your work

Access and Correction Requests

In general:	Best practices:
▪ Individuals have access to personal information about themselves. ▪ Individuals should be informed of the existence, use, and disclosure of their personal information and be given access to their personal information upon request, unless certain exceptions apply (e.g., providing information would increase risk of harm to an individual). ▪ Individuals can also challenge the accuracy of their personal information and request amendments or notes, as appropriate.	▪ Service providers who have custody and control of personal information should provide full records of personal information when the individuals requests access to it (unless there is a risk of harm or other exceptions apply). ▪ If a correction is requested and a change has been made to the personal information, service providers should transfer the amended information to third parties with whom the incorrect information was previously shared.

Now let's discuss access and correction requests.

In general, individuals have access to information about them. Individuals must be informed of the existence, use, and disclosure of their personal information. And, individuals must be given access to that information upon request, unless certain exceptions apply (e.g., if providing information would cause a risk of harm to an individual).

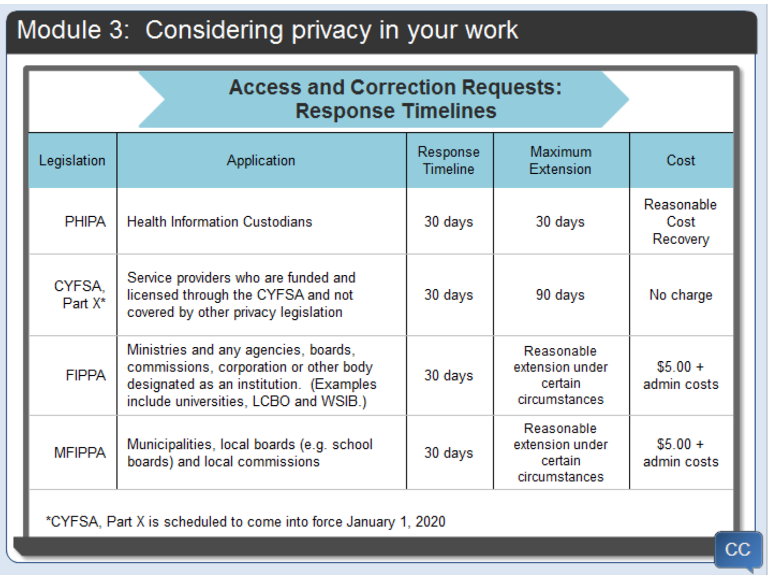
Individuals can also challenge the accuracy of their personal information and request amendments or notes, as appropriate.

Some best practices to keep in mind are:

A service provider, who has custody and control of personal information, should provide full records of personal information to the person who is requesting access (unless there is a risk of harm or other exceptions apply).

If a correction is requested and a change has been made to the personal information, service providers should transfer the amended information to their parties with whom the incorrect information was previously shared.

Response Timelines



Module 3: Considering privacy in your work

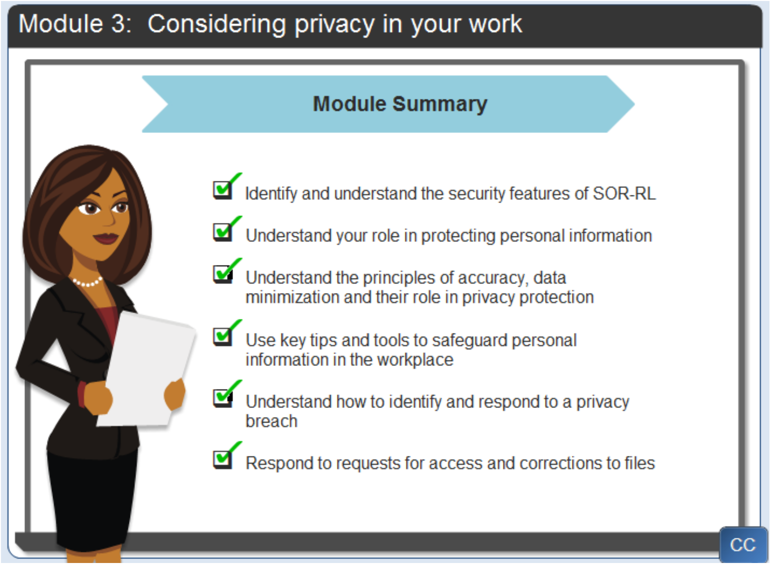
Access and Correction Requests: Response Timelines

Legislation	Application	Response Timeline	Maximum Extension	Cost
PHIPA	Health Information Custodians	30 days	30 days	Reasonable Cost Recovery
CYFSA, Part X*	Service providers who are funded and licensed through the CYFSA and not covered by other privacy legislation	30 days	90 days	No charge
FIPPA	Ministries and any agencies, boards, commissions, corporation or other body designated as an institution. (Examples include universities, LCBO and WSIB.)	30 days	Reasonable extension under certain circumstances	$5.00 + admin costs
MFIPPA	Municipalities, local boards (e.g. school boards) and local commissions	30 days	Reasonable extension under certain circumstances	$5.00 + admin costs

*CYFSA, Part X is scheduled to come into force January 1, 2020

This slide gives you a snapshot of each legislation's requirements and timelines for responding to access requests, possible extensions for responding, and costs that can be charged back to an individual for fulfilling an access request.

Module Summary



Module 3: Considering privacy in your work

Module Summary

- ☑ Identify and understand the security features of SOR-RL
- ☑ Understand your role in protecting personal information
- ☑ Understand the principles of accuracy, data minimization and their role in privacy protection
- ☑ Use key tips and tools to safeguard personal information in the workplace
- ☑ Understand how to identify and respond to a privacy breach
- ☑ Respond to requests for access and corrections to files

This concludes module 3.

I showed you how to identify and understand the security features of SOR-RL.

In this module you learned your role in protecting personal information.

You learned the principles of accuracy and data minimization.

You learned tips and tools to safeguard personal information in the workplace.

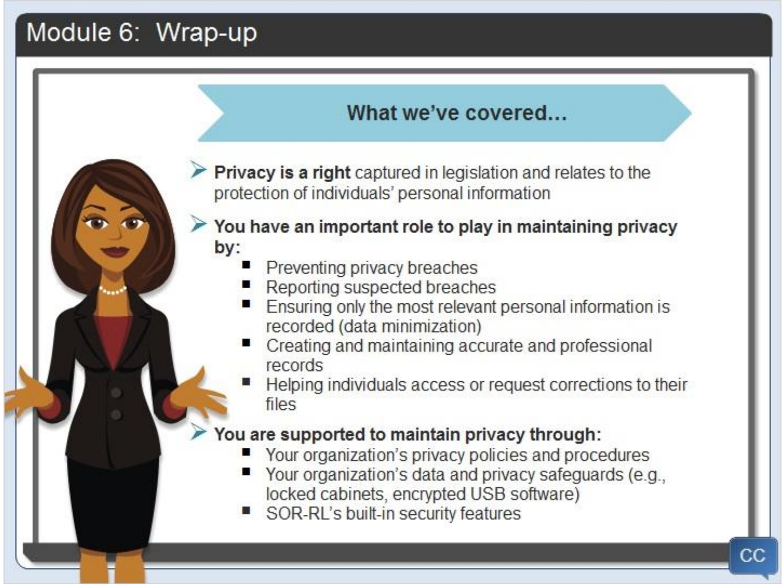
You understand how to identify and respond to a privacy breach.

And, you learned how to respond to requests for access and corrections to files.

Well done!

4. Module 4: Wrap-up

What we've covered



Module 6: Wrap-up

What we've covered...

- **Privacy is a right** captured in legislation and relates to the protection of individuals' personal information
- **You have an important role to play in maintaining privacy by:**
  - Preventing privacy breaches
  - Reporting suspected breaches
  - Ensuring only the most relevant personal information is recorded (data minimization)
  - Creating and maintaining accurate and professional records
  - Helping individuals access or request corrections to their files
- **You are supported to maintain privacy through:**
  - Your organization's privacy policies and procedures
  - Your organization's data and privacy safeguards (e.g., locked cabinets, encrypted USB software)
  - SOR-RL's built-in security features

In summary:

Privacy is a right captured in legislation and relates to the protection of individuals' personal information.

You have an important role to play in maintaining privacy by:

Preventing privacy breaches.

Reporting suspected breaches.

Ensuring only the most relevant personal information is recorded by following the principle of data minimization.

Maintaining accurate and professional records.

Helping individuals access or request corrections to their files.

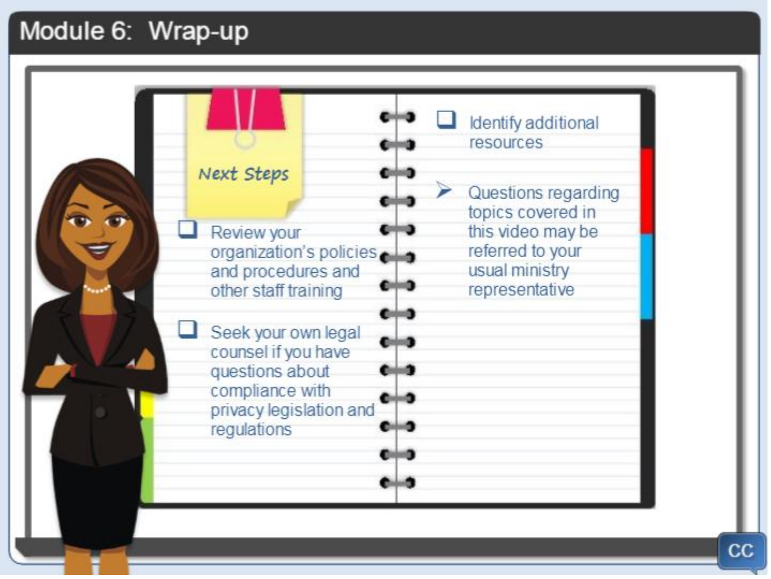
You should be supported to maintain privacy through:

Your organization’s privacy policies and procedures.

Your organization’s data and privacy safeguards (e.g., locked cabinets, encrypted USB key).

And SOR-RL’s built-in security features

Next Steps



Module 6: Wrap-up

Next Steps

- ❑ Review your organization’s policies and procedures and other staff training
- ❑ Seek your own legal counsel if you have questions about compliance with privacy legislation and regulations
- ❑ Identify additional resources
- ➢ Questions regarding topics covered in this video may be referred to your usual ministry representative

As next steps, we encourage you to:

Consider the privacy concepts and principles you’ve learned and review your organization’s policies and procedures and other staff training.

Seek your own legal counsel if you have any questions about whether or not you are in compliance with relevant privacy legislation and regulations.

Identify additional resources. For example, First Nations may have their own policies or rules for their communities. Check the band council website or ask your contact to confirm.

Questions regarding topics in this video may be referred to your usual ministry representative.

I hope to see you again soon!

Blank slide