Privacy Considerations for SOR-RL

Note: This presentation is intended for service providers reporting Serious Occurrences to the Ministry of Children, Community and Social Services (MCCSS). It must not take the place of legal advice. If you have questions about your privacy obligations, you should seek the advice of legal counsel.

Welcome to SOR-RL Training – Module 2

SOR-RL

- This training presentation is part of overall training to support the implementation and ongoing management of SOR-RL serious occurrence reporting requirements.
- There are four modules included in this training:
  - **Module 1** MCCSS SOR Guidelines
  - **Module 2** Privacy Considerations
  - **Module 3** Manual SOR Process
  - **Module 4** How to Use SOR-RL
- You are encouraged to complete each training module in the order shown above, and can access these modules at any time.

SOR-RL
Serious Occurrence Reporting - Residential Licensing

Training Products for Service Providers

Module 1: MCCSS SOR Guidelines

Guidelines + Key Enhancements Chart + Video

The Guidelines cover the purpose of SORs, business processes on who must report and when, and SOR categories and subcategories.

The Key Enhancements Chart and Video highlight changes to the Guidelines.

Module 2: Privacy Considerations

Presentation + Video

The Presentation and Video outline SOR-RL users' roles and responsibilities to protect personal information.

You are here!

Module 3: Manual SOR Process

Business Process + Video

The Business Process and Video outline how SORs will be submitted to the ministry if the SOR-RL online tool is temporarily unavailable.

Module 4: How to Use SOR-RL

Registration User Guide + User Guide + Video

The Registration User Guide explains how to register and log into SOR-RL. The User Guide and Video outline how to use the SOR module, with a focus on technical processes.

This is the recommended order to complete the modules. Parts of the modules can be revisited at any time.

Training Topics

- Personal information
- Relevant legislation / regulations
- Privacy principles
- Individual privacy rights
- Your role in protecting personal information
- Ensuring accuracy and upholding privacy
- Privacy breaches and safeguarding personal information
- Access and correction requests

Section One: General Privacy Concepts
What is Privacy and How Can it be Protected?

1) Privacy
2) Personal Information
3) Privacy Legislation Landscape
4) Privacy Rights
5) Privacy Principles

Section Two:
Considering Privacy in Your Work

1) Your Role in Protecting Privacy
2) Ensuring Accuracy and Upholding Privacy
3) Privacy Breaches and Safeguarding Personal Information
4) Access and Corrections Requests

Section One: General Privacy Concepts *What is Privacy and How can it be Protected?*

Learning Objectives

- Define privacy
- Understand why it's important to protect the privacy of personal information
- Identify and describe the current environment of privacy legislation in Ontario
- Define and recognize personal information

What is Privacy?

SOR-RL

- Privacy has different dimensions
  - *Territorial Privacy* – space or location free from intrusion, historically related to the home
  - *Personal Privacy* – freedom of movement and expression, right to personal space
  - *Information Privacy* – individuals have control and ownership over their information (e.g., medical history, birth dates, banking information)

- This training focuses on **Information Privacy**
  - Individuals determine when, how and to what extent information about themselves is communicated and used

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

Helps us be ourselves

Be a Canadian societal right

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

Privacy Rights

In Ontario, legislation generally provides individuals with the right to:

1. **Consent** to the collection, use, and disclosure of their personal information*
2. **Know why and how** their personal information will be collected, accessed, stored, and disclosed
3. **Have reasonable access** to information kept about them
4. **Be informed about privacy breaches** and actions taken to correct or mitigate the breach
5. **Request corrections** or notes to their records
6. **Make a complaint** to a relevant body*

*Please refer to Appendices A and B for more information

You have a key role in upholding individuals' privacy rights

Privacy Legislation Landscape

SOR-RL

Privacy Principles

Underpin privacy legislation.

Help to uphold privacy rights to protect individuals from harm:

Accountability

Accuracy

Transparency / Consent

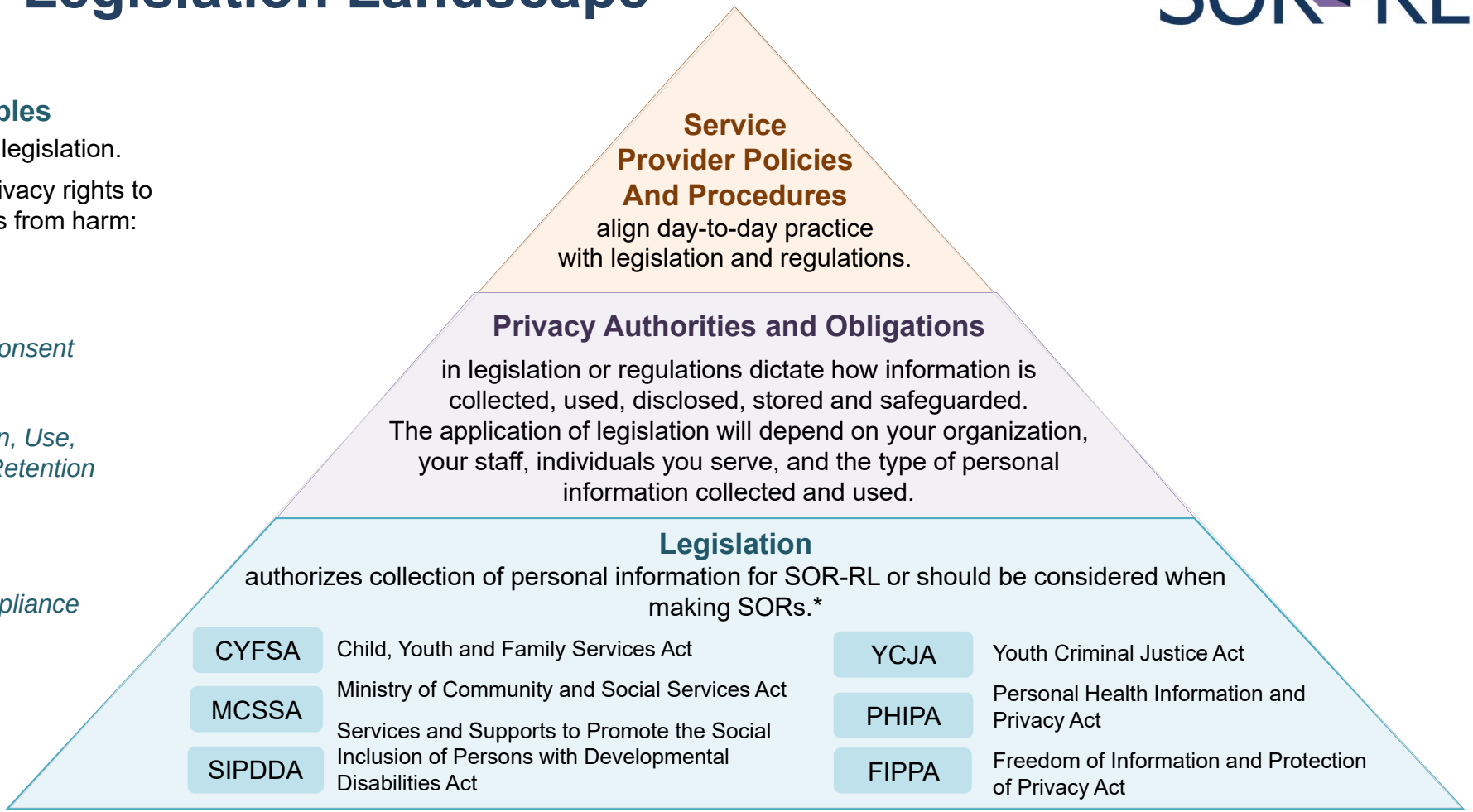
Individual Access

Limiting Collection, Use, Disclosure, and Retention

Openness

Safeguards

Challenging Compliance



*See Appendix A for further context and detail

What is Personal Information?

Any recorded information that could lead to the **identification of an individual.**

It's important to recognize personal information when you see it so you can protect it through appropriate collection, use and disclosure, as well as through using the appropriate safeguards and information management practices.

Ask yourself: *Is it reasonable to expect someone could be identified from the information?*

Remember! Context is important.

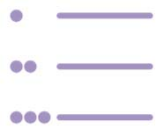
Personal information is not only about if you personally could identify the individual with the information you have, but if others could given their knowledge and background.

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

Test Your Understanding! (Personal Information)

SOR-RL

Which cases would include personal information?



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 but had address and birth date information, 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.

Test Your Understanding!
(Personal Information Scenarios)

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

1. Zack Individual 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.

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

2. Carol Individual is female, identifies as Black and lives in ABC group care home in Toronto. She is the only female in the home.

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

Test Your Understanding!
(Personal Information Scenarios – ANSWER KEY)

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

1. 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.

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

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

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

Section Two:
Considering Privacy in Your Work

Learning Objectives

- 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 a privacy breach and best practices for responding to a privacy breach
- Respond to requests for access and corrections to files

Security Features of SOR-RL

The Ministry of Children, Community and Social Services (MCCSS) is improving processes for SO 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 SO 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, the SOR-RL system has the following built-in security features to support the safeguarding of information:

Technical 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 of individuals involved
- Multiple firewalls will help prevent unauthorized access
- SOR-RL has been tested for vulnerability and penetration

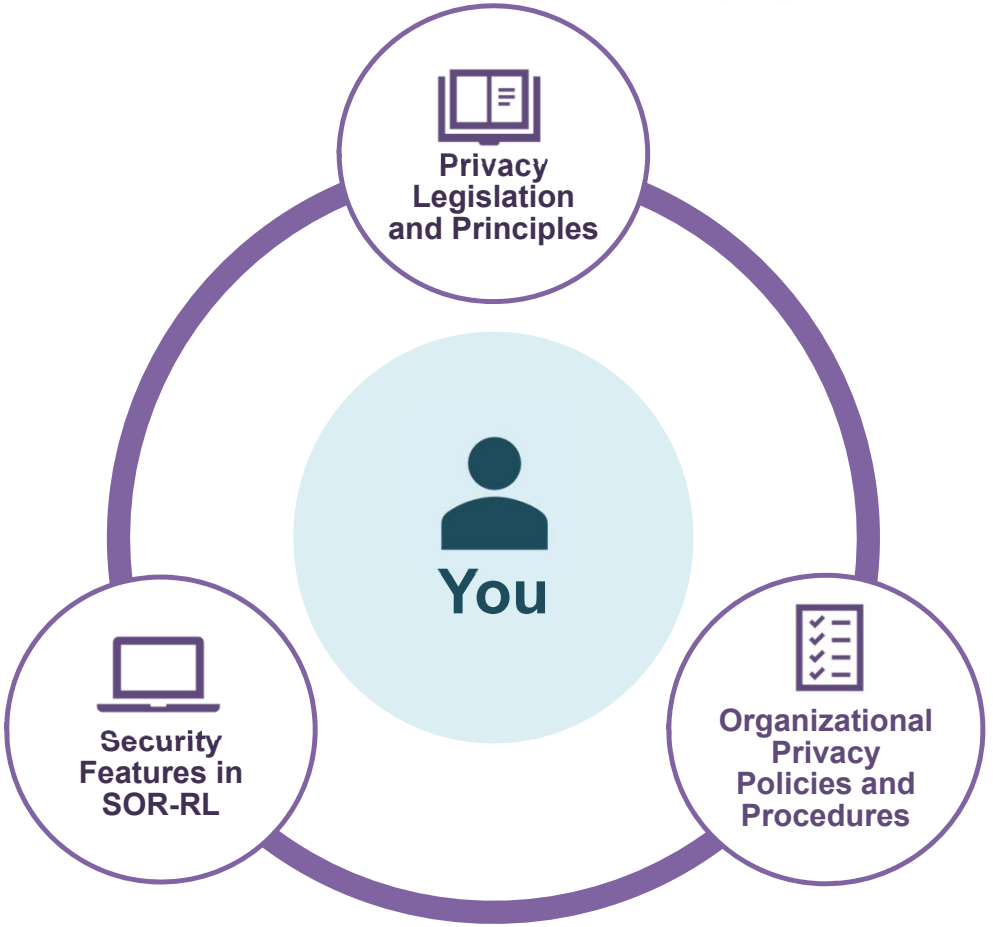
Access Features

- 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
  - Random, one-time-passwords delivered to user's email address for each login
- Access to information in SOR-RL is based on assigned user roles
- Staff are limited to access SORs for their site location only.
- At time of login, users are reminded that it is fraudulent to use another person's account
- User activity logs will track how information is stored and accessed for auditing purposes

Your Role in Protecting Personal Information

SOR-RL

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.



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. Data minimization was an important consideration in the creation of SOR-RL.

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

How do I practice 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).

For example

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 should the worker include?

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

What should the worker omit?

- 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

*Please see the MCCSS SOR-RL Guidelines 2019 for more information on completing SORs.

Accurate and Professional Note-Taking

It is important to keep in mind both your purpose for making a Serious Occurrence (SO) and that individuals have a right to access their information.

As such, you should make efforts to ensure that personal information included in reports is **accurate** and **professional**.

Best practices include:

- 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 / perspective in the SOR

Accurate and Professional Note-Taking for SORs

It is important to remember the purposes for making an SOR. It is a process that:

- Allows service providers to manage incidents as they occur, make records of the incidents, and monitor actions taken in response to incidents in order to prevent or mitigate future incidents
- Supports MCCSS in monitoring and overseeing service providers in the delivery of services

SOs 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?

- A privacy breach is when personal information is:
  - Lost or stolen
  - 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 with personal information on it
  - **Sending personal information to the wrong recipient:** emailing files with personal information to someone who doesn't have the authority to receive the information or having a conversation involving personal information where others may overhear
  - **Hacking** an electronic database containing personal information (e.g., ransomware attack)

Safeguarding Information: Preventing Privacy Breaches

- **Secure information starts with you!** As a person delivering services, you should consider taking reasonable steps to protect personal information. The following tips will help you ensure information isn't disclosed or used without permission, lost or stolen:

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 discs, 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

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

Use Your Judgement

- Know and follow your organization's privacy policies and procedures
- Consider risks to privacy when accessing, disclosing, discarding or transferring personal 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 for Organizations to Safeguard Personal Information

SOR-RL

Does your organization have the right tools 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

Test Your Understanding! (preventing Privacy Breaches)

Karen was drafting an SOR and was about to take a washroom break. She wanted to pick up right where she left off after she got back, so instead of locking her computer, she simply turned off her monitor and closed the cover on the files on her desk. She was only going to be gone for five minutes after all!

Later that day, Karen ran into her colleague who was also working on a separate SOR at 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.

- **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?**

Test Your Understanding!
(Preventing Privacy Breaches: Answer Key)

SOR-RL

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.

What happened or could have happened as a result?

- 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 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.

Test Your Understanding!
(Preventing Privacy Breaches: Answer Key Part 2)

SOR-RL

How can Karen improve her practices going forward?

- Sign out of SOR-RL on her computer, lock the screen, or another action that ensures only individuals with a password can 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.

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.

Responding to Privacy Breaches

SOR-RL

Despite best efforts, privacy breaches may still occur. It is a best practice to establish protocols for responding to privacy breaches. Here are some key steps and considerations that should inform privacy breach responses.

1) Respond and Contain

a. **Report** all suspected breaches to a supervisor or manager, and other authorities as necessary.
   a. **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. (See details on slide 29).

b. **Assess and determine:**
   a. If a breach has occurred
   b. The sensitivity of the breached information
   c. If it is an isolated incident, ongoing or recurring
   d. The number of individuals affected
   e. Potential harms to affected individual(s), the institution and public

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

Responding to Privacy Breaches (Part 2)

2) 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.

Note: This is a requirement for service providers who are subject to **PHIPA and CYFSA Part X** (scheduled to come into effect January 1, 2020).

3) 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.

4) Implement Change

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

Reporting Privacy Breaches in SOR-RL

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 a SOR within 1 hour of becoming aware of the SO or deeming the incident to be an SO.

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

Remember: 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.

Refer to the SOR Guidelines for more information.

Access and Correction Requests

In general, individuals should 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 may also challenge the accuracy of their personal information and request amendments or notes, as appropriate.

Best Practices:

- 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.

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, commisions, corporation or other body designated as an institution (Examples include universities, LCBO and WSIB)	30 days	Reasonable extension under certain circumstances	$5.00 + administrative costs
MFIPPA	Municipalities, local boards (e.g. school boards) and local commissions	30 days	Reasonable extension under certain circumstances	$5.00 + administrative costs

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

What We've Covered

SOR-RL

- **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 through:**
  - 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 by:**
  - Your organization's privacy policies and procedures
  - Your organization's data and privacy safeguards (e.g., locked cabinets, software)
  - SOR-RL's built-in security features

Next Steps

1. Consider the privacy concepts and principles you've learned and review your organization's policies and procedures and other staff training
2. Seek your own legal counsel if you have any questions about whether or not you are in compliance with relevant privacy legislation and regulations
3. Questions regarding topics covered in this training may be referred to your usual ministry representative
4. Identify additional resources
   - For example, First Nations may have their own policy policies or rules for their communities - check the band council website or ask your contact to confirm.

APPENDIX A: Privacy Legislation Landscape

Legislation	Who it applies to	How it Affects SOR-RL / considerations
Freedom of Information and Protection of Privacy Act (FIPPA)	General privacy requirements for provincial government institutions • (e.g., ministries, agencies, universities)	Allows any individual to request access to information kept by government and institutions, including any personal information.
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)	Local government organizations • (e.g., school boards)	Allows individuals to request access to information kept by local government organizations, including personal information.
Personal Health Information and Privacy Act (PHIPA)	Health Information Custodian • (e.g., hospitals, health practitioners)	PHIPA outlines the purposes and direction for collecting, using, and disclosing personal information in the health sector. Health information should be handled per the direction specified in PHIPA.
Youth Criminal Justice Act (YCJA)	Youth justice system entities • (e.g. custody/detention facilities)	The YCJA protects the privacy of young persons in conflict with the law by restricting the publication of information that would identify those young persons, in addition to witnesses or victims of youth crime who are under age 18. The YCJA also provides strict limitations on the access to, and disclosure of records about young persons that are kept under the Act. The YCJA is federal legislation, and therefore takes precedence over provincial legislation if there is a conflict. Your organization is required to comply with the YCJA regarding a young person's information and records.
Child, Youth and Family Service Act (CYFSA)	Funded service providers, child welfare agencies, residential licensees, and some foster parents	Part X outlines the purposes and direction for collecting, using, and disclosing personal in the child, youth and family services sector.
Ministry of Community and Social Services Act (MCSSA)	The ministry and funded service providers • (e.g., women's shelters, residential Indigenous Healing & Wellness service providers)	Transfer Payment Recipients receiving funds to implementing programming that is subject to the MCSSA must abide by privacy requirements outlined in the Act and service contracts.
Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act (SIPDDA)	Funded service providers • (e.g., intensive support residences, placing / case management agencies)	Authorizes direct and indirect collection of personal information from individuals who apply for or receive services and supports from service agencies or direct funding. Part VIII outlines how personal information is collected and used under the Act.

Questions? Seek advice from legal counsel on how legislation impacts your work.

APPENDIX B: Privacy Principles (Part 1)

SOR-RL

Accountability

- All staff are responsible for the security and confidentiality of personal information under their control
- Organizations and staff must help inform and support individuals to make access requests, complaints or challenges
- The organization is responsible for creating policies and procedures that ensure personal information is collected, used, disclosed, and retained in a manner that upholds individuals' privacy rights

Accuracy

- All staff are responsible for providing accurate, complete, and up-to-date information
- SORs should be recorded and reported in a professional manner (i.e., avoid non-factual commentary unless specified it's an individual's view / perspective)

Transparency / Consent

- Individuals and / or their guardians should be informed that their personal information will be shared with the ministry as part of the SO reporting process for system planning and oversight purposes.

Individual Access

- Individuals have a right to access their files and information about them, unless there are significant safety concerns or a law and / or court order prevent it
- Staff should be prepared to respond to access requests within legislative timelines and prepare files with access in mind (i.e., take professional notes, ensure accuracy of information)

APPENDIX B: Privacy Principles (Part 2)

SOR-RL

Limiting Collection, Use, Disclosure, and Retention of Information

- The information staff include in an SOR should be limited to what is absolutely necessary to serve the intended purpose
- Organizations should consider privacy when creating their policies and practices around use, disclosure and retention of records

Openness

- Organizations should make information about how they manage personal information public and readily available to individuals.

Safeguards

- The SOR-RL system has many security measures in place to help protect information; however, you have a role and responsibility to help further protect personal information. For example:
  - Limiting access to SOR-RL and confidential files
  - Using strong passwords for accounts
  - Exercising caution when handling sensitive information to ensure others can't see your screen or hear your conversations

Challenging Compliance

- Individuals have the right to challenge compliance.