SOR-RL Business Processes Tip Sheet

Subject	Tip
Privacy Considerations	
Privacy: Key Messaging that service providers can incorporate into information for individuals who are accessing their supports regarding the collection of Personal Information (PI) in Serious Occurrence Reports and entered in SOR-RL.	**Protecting the privacy of individuals is very important to the ministry (and to the service provider).** Only authorized ministry employees, and service provider staff that have been security screened will have access to PI and that access will be tracked and monitored to prevent unauthorized access, use or disclosure. PI collected in SOR-RL will be used to: • Improve program quality and integrity (e.g. identify duplicate or linked records). • Improve service delivery (e.g. support connecting individuals to complementary services and/or improve transitions between program). • Support program analysis, planning and research from a system view by identifying common trends and patterns in de-identified cases (e.g. identify potential opportunities to support future clients and drive better outcomes. According to the Ontario Chief Coroner, the circumstances of an individual may be influenced by their intersections with various government systems throughout the course of their life. Understanding these intersections could provide insight into potential intervention points in the interest of public health and safety.
Privacy Technical Safeguards	Recording personal information of clients involved in SORs has been an existing practice in place since the start of reporting. As part of government policy and IT development for SOR-RL, the nature of personal information collection was reviewed extensively. SOR-RL was designed with significant technical safeguards, including encryption, audit controls, system security and two-factor authentication of all users. o **For programs administered by Violence Against Women (VAW), Provincial Anti Human Trafficking Coordination Office (PATCO) and Indigenous Healing and Wellness (IHWS)**: shelter addresses are not collected by the ministry and do not appear in SOR-RL to protect the location of clients who may be involved in an SOR. In exceptional circumstances, some service providers may not have access to or be able to share information that is requested. In these exceptional circumstances the PI entered in SORs may be limited to initials and date of birth rather than full first and last name and date of birth. Ministry approval is required to limit PI information for program areas.

Subject	Tip
Privacy Training	In addition to robust technical safeguards, the ministry is providing privacy training as part of its online suite of training materials for internal and external users. This training is intended to inform operational policies and practices of service providers to further enhance the technical protocols already in place.
Privacy: Purpose of collecting PI in SOR-RL	MCCSS mandate is to provide the children, youth and adults we serve the best opportunity to succeed and reach their full potential. As a demographic, these individuals are some of the most vulnerable people in Ontario and they cross multiple programs and service providers. SOR-RL is about the safety of the most vulnerable children, youth and adults in this province. Every day, children, youth and vulnerable adults are supported by service providers and may be involved in serious occurrences. SORs are prescribed reports submitted to the ministry serving as a key monitoring and oversight tool of service delivery. Our current manual licensing and SOR processes limit our ability to get complete, accurate, and timely data that can serve as early warning signs. The existing business process relies on fax and emailed transmissions of SORs and licensing documents from service providers to ministry offices. The existing process limits provincial level data to inform risk assessment, conduct policy development and operational planning and undertake trend analysis. The ministry requires the ability to link data for operational and business intelligence. The current process limits the ministry's ability to adopt a risk-based issues management and licensing approach to improve oversight. Our service providers have asked for more efficient ways to be able to comply with ministry's reporting requirements while protecting the privacy of the individuals they serve. SOR-RL is a tool that has been designed with that need in mind. SOR-RL data will be linked, analyzed and made available to service providers and the ministry to support system planning and oversight, contributing to better outcomes for children, youth and vulnerable adults. The training on Privacy Considerations in SOR-RL web portal will help you understand how the identity of individuals will be protected. Legislation gives the ministry and its service providers a legal framework for collecting using personal information (see the 2019 SOR Guidelines for information around the relevant legislation: CYFSA, YCJA, MCSSA, SIPPDA, PHIPA, FIPPA).

Subject	Tip
Privacy: Who will have access to PI that is entered in an SOR?	See the Privacy Considerations training module regarding the limitations and protections of personal information. Service providers have policies and procedures regarding the collection and sharing of personal information. They have a responsibility to inform the individuals they serve of the information they will be collecting and with whom it will be shared. Only authorized ministry employees, and service provider staff that have been security screened will have access to PI and that access will be tracked and monitored to prevent unauthorized access, use or disclosure.
Privacy: Is the PI (records) in an SOR subject to a subpoena by the court?	Information that is collected in an individual's client record, including SORs, may be requested by the court. Service Providers and MCCSS would need to provide information that is requested through court orders. The information within SOR-RL may be required by a subpoena or court order. The information about individuals that is gathered in the existing manual SOR process has been subject to the same requirements. The 2019 MCCSS SOR Guidelines and introduction of SOR-RL has not changed that requirement.
Privacy: Submitting an SOR: Service Provider SOR Approval	If a service provider's internal policy requires management's approval on SOR submissions, the manager's name may be added to the SOR before it is submitted to the ministry. See section **3.3.10** in the SOR Reporting Guide with the option of including the name of who approved it.
Privacy: Printing SORs	Printed or PDF copies of SORs from SOR-RL will redact (hide) names and dates of birth.
Changes to reporting timelines	
Reporting Timelines: When a serious incident happens after hours, and I need to report it to the ministry what do I do?	The SOR Guidelines define the timelines for reporting SORs to the ministry. The Key Enhancements #2 provides more information around Level 1 and Level 2 reporting. Please refer to that document for more detail. SORs should be submitted to the ministry through SOR-RL. If SOR-RL is unavailable, there is a manual SOR process in place. For Youth Justice service providers, any Level 1 SOR requires an immediate phone call to the ministry and a SOR within one hour. That practice has not changed with the updated 2019 SOR Guidelines or introduction of SOR-RL. For non-YJ providers only, the ministry considers the immediate notification and submission of a SOR within 1 hour to be the same. The immediate

Subject	Tip
	notification/1hour report submission by non-YJ service providers should be within SOR-RL and does not require a phone call or email to a designated ministry contact. SOR-RL will notify appropriate parties when the SOR is submitted. The ministry will monitor the receipt of SORs and follow up directly with the service provider if additional information is needed.
What happens if an SOR is reported outside the timelines?	The service provider's priority should always be to attend to the health and safety of individuals involved in the incident and stabilize the incident before submitting an SOR. If the service provider is unable to provide the ministry with information about Level 1 serious occurrences within the 1 hour reporting time frame, service providers can explain why the report is submitted outside the time frame by entering comments within the SOR submitted. The ministry will work with services providers to understand why the SOR was submitted outside of the reporting time frame; the intent is not to penalize service providers who submit reports outside the Guidelines time frames. For the Level 1 initial SOR submission, service providers should try to provide as much information about the SO as they can, but the Level 1 submission can be added to once more information becomes available and the service provider is able to provide more details. As we implement the timeline changes for non-YJ service providers, the ministry will work with service providers to understand and evaluate the impact of this change. The new reporting time frame for non-YJ service providers will allow the ministry to have timely information about incidents that require urgent attention. If service providers are unsure whether the incident is a Level 1 or Level 2 serious occurrence, the service provider should contact their designated MCCSS contact(s) for assistance.
Service Provider accessing data from SOR-RL	
General SOR-RL question: SOR information use by service providers	The Service Provider Administrator (LRA) can access SOR information for all sites that their organization operates.
General SOR-RL question: Exporting SORs Information / Integration	Service providers may use search function to locate individual SORs. Due to the sensitivity of information, SOR data cannot be exported from SOR-RL. Integration with case management systems (at the ministry or a service provider) is not in scope for the project.

Subject	Tip
with other systems	
General SOR-RL question: Old/existing SOR Information	When SOR-RL launches, all new SOR's are required to be submitted using SOR-RL (or in the event the system is unavailable the SOR is to be submitted following the Manual SOR Business process. SOR information from previous systems (SOS, YJSOI) will **not** be migrated to SOR-RL. The ministry will maintain the SOR records within these legacy systems. Service providers should maintain SOR records that occurred prior to SOR-RL following their existing file/record retention policy. SOR's submitted prior to SOR-RL's launch will need to be monitored, updated following the reporting processes that were in place at the time of the incident, until they are closed for no further action. Service providers should continue to fax in or email the updates for these SORs that precede SOR-RL following the format associated with the 2013 SOR Guidelines, and the 2008 YJ SOR Manual as indicated. SOR information (that has been entered into SOR-RL) will be available to service providers to access through the system to inform their own risk management and planning about individuals.