

# Harm Reduction Data Base Project - Privacy Impact Assessment

**Privacy Reviewer: Samara Starkman, Drawbridge Consulting Inc.**

**Review Date: October 20th, 2017**

**Name of the organizations involved:** CAMH, Ministry of Health and Long-Term Care (MOHLTC), Positive Living Niagara (StreetWorks needle exchange), Sanguen Health Centre, Peel Works Needle Exchange Program, Kingston Community Health Centres, Street Health Centre, Lambton Public Health

**Name of organization or HIC with responsibility for system or service:** CAMH

<b>Project Summary:</b>	
<b>Project Name:</b>	<b>Harm Reduction Database Project</b>
<b>Sponsor(s):</b>	Karen McConn
<b>Project Manager:</b>	Susan Allen
<b>Organization(s) implementing project:</b>	CAMH
<b>Estimated Go-live:</b>	Pilot: Planned for October 2017, Full Go-Live: Unknown

## **Acronyms:**

**CAMH:** Centre for Addiction and Mental Health

**ONHRDB:** Ontario Harm Reduction Database

**HRHSPs:** Harm Reduction Health Service Providers

**MOHTLC:** Ministry of Health and Long-Term Care

## **Executive Summary:**

The goal of the Ontario Harm Reduction Database (ONHRDB) initiative is to implement a comprehensive harm reduction service management and reporting system that meets the needs of harm reduction programs funded by the Ministry of Health and Long-Term Care (MOHLTC). The data collected through this system will help service providers manage their programs, increase the ability of decision-makers to monitor and analyze trends, as well as provide a tool for efficient and standardized data collection and inventory control. CAMH, in partnership with the MOHLTC and NEO360 (the vendor), will implement the OHRDB at selected sites in Ontario offering publically-funded harm reduction programs. The initial implementation at five (5) pilot sites is scheduled to begin in October.

## Harm Reduction Data Base Project - Privacy Impact Assessment

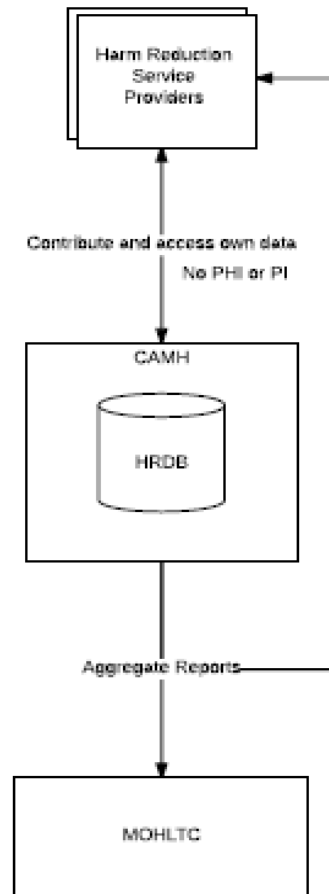
The technology that will be used for the HRDB is called “NEO”. NEO is a commercial off the shelf (COTS) web-based application used by harm reduction health service providers (HRHSPs) for service management and reporting. NEO will be used by HRHSPs to record information about the service provided and supplies administered through the provincial harm reduction programs, including: Needle Exchange Programs (including their respective mobile needle exchange sites), Hepatitis C teams, and Injection Drug Use Outreach Programs. **No Personal Health Information or Personal Information will be collected, used and/or disclosed.**

Despite the fact that this initiative is not intended to collect, use and/or disclose personal health information or personal information, a privacy impact assessment (PIA) has been undertaken to ensure that potential data risks involved in this initiative are identified and mitigated. This PIA uses the 10 Fair Information Privacy Principles in order to assess such risks. The scope of this PIA is limited to the pilot. If PHI or PI is to be collected for the full go-live, an additional PIA should be conducted.

Four risks and five recommendations have been identified. The risks are medium or low given the nature of the data involved in this initiative.

# Harm Reduction Data Base Project - Privacy Impact Assessment

## Data Flow



# Harm Reduction Data Base Project - Privacy Impact Assessment

## Privacy & Security Summary

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
<p><b>1. Accountability &amp; Governance</b></p> <p><i>Any organization is responsible for PHI in its possession or custody.</i></p> <ul style="list-style-type: none"> <li>• Designated contact &amp; delegates?</li> <li>• Oversight processes?</li> <li>• Agreements?</li> <li>• Contracts with third parties?</li> <li>• Program specific policies?</li> <li>• Monitoring/auditing?</li> <li>• Training?</li> </ul>	<p>For the HRDB Pilot and subsequent operations of the HRDB, CAMH is operating as a service provider. It is also acting as an Agent (as that term is defined in PHIPA) of the HRHSPs in that it is providing reporting to the MOHLTC on behalf of the HRHSPs. In accordance with the agreement entered into with the MOHLTC, CAMH has entered into an agreement with NEO360 for the license of a comprehensive harm reduction service software solution (i.e. The Ontario Harm Reduction Database), to be hosted by CAMH for use by the HRHSP's for the supply management and reporting obligations.</p> <p>An agreement has been entered into between CAMH and the vendor, NEO 360. CAMH has not yet entered into an agreement with each of the sites. CAMH will enter into agreements with each of the pilot sites.</p> <p>There is a Steering Committee and an Advisory Group for this initiative. Each has defined terms of reference, and the draft Service</p>	<p>1. CAMH has not yet entered into an agreement with each of the pilot sites. The draft is being reviewed at the time of writing this PIA. CAMH will enter into agreements with each of the pilot sites.</p> <p><b>Risk Rating: Medium-High</b></p>	<p>1. Enter into an agreement with each of the pilot sites.</p> <p>2. If NEO is to provide training directly to HRHSPs, ensure that any agents are appropriately trained on privacy procedures.</p>

## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
	<p>Provider Agreement outlines the data decision making governance regarding data under section 5. CAMH cannot make these decisions independently as it is acting as a service provider. CAMH will monitor the use of the system, including auditing and IT maintenance. Tier 2 support may be provided by NEO360 but NEO will not have access to personal information.</p> <p>CAMH staff will follow existing CAMH Policies as well as any new policies and procedures that may be developed by the Steering Committee.</p> <p>Training on the NEO system may be provided by NEO. Participating agencies are responsible for ensuring that they have appropriate privacy training.</p>		
<p><b>3. Identifying Purposes</b></p> <p><i>The organization shall document the purposes for which PHI is collected at or before the time of collection.</i></p> <ul style="list-style-type: none"> <li>• Purposes are fulsome?</li> <li>• Purposes published?</li> </ul>	<p>No PHI will be collected for this initiative. Should PHI be collected in the future, this PIA should be amended accordingly.</p>	<p>N/A</p>	<p>N/A</p>
<p><b>4. Consent</b></p>	<p>Because no PHI will be collected</p>	<p>N/A</p>	<p>N/A</p>

## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
<p><i>Patient consent is required for the collection of PHI and the subsequent use or disclosure of this information.</i></p>	<p>for this initiative, consent is not required. Unique identifiers will be used for each client, however, consisting of the first two letters of first name, last two letters of last name, year of birth and a gender identifier. Should a client not wish to provide his/her initials or birthdate, an anonymous identifier may be created by the User. Each HRHSP is responsible for being open and transparent as per their regular practices for informing clients about the data collected and reported regarding services used. Also refer to the section on Openness in this PIA table. One site will not have access to the data of another site.</p>		
<p><b>5. Limiting Collection</b></p> <p><i>Organizations shall not collect PHI indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified.</i></p> <ul style="list-style-type: none"> <li>• Limited data?</li> </ul>	<p>The Steering Committee has approved a minimum data set, which will form the basis of the collections. Fields that may include sensitive information (such as year of birth or gender), can be completed with fake data if the client does not want that detail provided. There will be no PI or PHI collected.</p>		

## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
<p><b>2. Limiting Use, Disclosure &amp; Retention</b></p> <p><i>Organizations using PHI for a new purpose shall document this purpose and only disclose for purposes that are consented to. Organizations should develop guidelines and implement procedures with respect to the retention of PHI. PHI that is no longer required to fulfill the purposes should be destroyed, erased, or made anonymous.</i></p>	<p>Each HRHSP shall provide certain data concerning services delivered to clients who access, participate in, and/or are reached through the provincial harm reduction programs, including Needle Exchange/Syringe Programs (including their respective satellite/mobile needle exchange sites), Hepatitis C Programs, and Injection Drug Use Outreach Programs as further set out in an agreement or as otherwise required by the Harm Reduction Steering Committee.</p> <p>CAMH will provide regular reports to HRHSPs and the MOHLTC as further described in the agreement. Each HRHSP will be able to access their own data through a user-based web portal accessible to users from any location with internet access. HR HRP's will be able to make queries (about only their own data) through the portal.</p> <p>The HRDB will also allow for certain coordination of supplies by the Ontario Harm Reduction Distribution Program, a centralized inventory management system, which will have access to the database to</p>	<p>N/A</p>	<p>N/A</p>

## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
	<p>enable a more efficient order management process for harm reduction products.</p> <p>There is no PHI or PI contained in the data submitted to CAMH, however, in the event the at PHI or PI is inadvertently submitted to the HRDB, CAMH shall de-identify data prior to sending any reports to any HRHSP or the MOHLTC to ensure that any such reports do not contain PHI..</p> <p>CAMH shall provide the de-identified data to the MOHLTC through a designated portal created by CAMH.</p> <p>CAMH will delete data upon request of the HRHSP that provided that data. If not directed to delete the data, it will be retained by CAMH for as long as required to meet the specified MOHLTC purposes. Any reports derived from the data will be retained according to CAMH's internal data retention policies.</p>		
<p><b>3. Accuracy</b></p> <p><i>Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility</i></p>	<p>It is the responsibility of the sites entering the data to ensure that the data is as accurate as possible.</p>	<p>N/A</p>	<p>N/A</p>



## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
<i>that inappropriate information may be used to make a decision about the individual.</i>			
<p><b>4. Safeguards</b></p> <p><i>The security safeguards shall protect PHI against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect PHI regardless of the format in which it is held.</i></p> <ul style="list-style-type: none"> <li>• TRA?</li> </ul>	<p>A TRA is being performed on the HRDB. This report is not yet complete; it will be completed following NEO configuration. The Server OS hosting the data will be backed up nightly, and the MS SQL Server database used by NEO will be using transaction log backups and as such, the data will be backed multiple times per day. Backups will be stored in the CAMH Backup and Disaster Recovery host, Sungard. The draft Service Provider Agreement provides for technical, administrative and physical safeguards in an appendix.</p>	<p>2. There is a risk that the data is not secure if the TRA is not complete and the recommendations are not followed prior to implementation. <b>Risk Rating: Medium</b></p> <p>3. CAMH must ensure that it has the safeguards in place as specified in the agreement or risk breaching that agreement while putting potentially sensitive data at risk. <b>Risk Rating: Medium</b></p>	<p>3. Ensure the TRA is completed and risks mitigated prior to go-live.</p> <p>4. Verify compliance with safeguards specified in the draft Service Provider Agreement prior to go-live.</p>
<p><b>5. Openness</b></p> <p><i>Organizations shall be open about their policies and practices with respect to the management of PHI. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort.</i></p>	<p>No PHI or PI is collected through this project. Nevertheless, it is the responsibility of the sites to ensure that they are open with their clients regarding how the information collected will be used, if requested.</p>	<p>4. There is a risk that sites will be unable to communicate to clients regarding the purposes for collecting information for the HRDB. This is not a high risk as consent is not required for collecting the data. <b>Risk Rating: Low</b></p>	<p>5. Create communications materials for sites to enable better communication about the HRDB. This may form a part of the training materials.</p>
<p><b>6. Access</b></p> <p><i>Upon request, the organization</i></p>	<p>As data is not identifiable, clients will not be able to access their information.</p>	N/A	N/A

## Harm Reduction Data Base Project - Privacy Impact Assessment

CSA Principles	Compliance Status & Current Controls	Outstanding Risk	Recommendation
<p><i>shall inform an individual whether or not they hold PHI about that individual.</i></p>			
<p><b>7. Challenging Compliance</b></p> <p><i>Organizations shall put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of PHI. Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.</i></p>	<p>Sites are responsible for responding to inquiries or complaints about their own compliance with applicable laws and regulations.</p> <p>With respect to the operation of the HRDB, CAMH policies and procedures apply.</p>	N/A	N/A

# Harm Reduction Data Base Project - Privacy Impact Assessment

## Appendix A: Risk Rating Description

Privacy risk to the organization is assessed based on a combination of impact of the risk should it manifest versus likelihood of the risk occurring.

The impact of a risk becomes higher if:

- (1) the issue or event is contrary to legislative or contractual rights or obligations
- (2) involves a previously published regulatory order, or
- (3) involves an increasing number of patients or CAMH agents.

The likelihood of a risk is assessed based on:

- (1) the previous history of the risk occurring,
- (2) perceived gaps that would increase the likelihood of the risk manifesting.

**Risk Rating Grid**

<b>High</b>	<b>Impact</b>	<b>Medium</b>	<b>High</b>	<b>High</b>
<b>Medium</b>		<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>Low</b>		<b>Low</b>	<b>Low</b>	<b>Medium</b>
		<b>Likelihood</b>		
		<b>Low</b>	<b>Medium</b>	<b>High</b>