March 23 2017

CanROC
Canadian Resuscitation Outcomes Consortium
Consortium Canadien de Recherche en Réanimation

CanROC Registry and Database Risk Assessments

The Canadian Resuscitation Outcomes Consortium is a national initiative handling sensitive data across a range of complex relationships between academic institutions, hospitals, and emergency services. Due to these complexities, the CanROC research team and St. Michael's Hospital, which houses the CanROC database, underwent an external privacy and security audit prior to the launch of data collection.

THREAT RISK ASSESSMENT

The Threat Risk Assessment (TRA) is a critical exercise for ensuring protection of electronic data for all CanROC patients. The focus of the TRA was identifying any potential vulnerabilities related to data and operational security. Specific items in scope included: network architecture, web and database servers, workstations, firewalls, security configurations, disaster recovery and backup planning, and policies and procedures related to system administration and governance. Data was collected through surveys, interviews, vulnerability scans and penetration testing.

The TRA found the CanROC system to be "Average" compared to similar organizations and systems, and provided recommendations related to three major risk categories:

- Application vulnerabilities, related to the CanROC database website
- Infrastructure vulnerabilities, related to the systems and hardware at St. Michael's Hospital
- Incidental vulnerabilities, related to CanROC and St. Michael's Hospital policies and procedures

After receiving the TRA report, the CanROC research team worked with St. Michael's Hospital Information Technology staff, and members of the Applied Health Research Centre to develop an action plan and implement the recommendations made in the TRA. Often, not all recommendations will be possible to implement, and certain recommendations may require long-term solutions over a period of several years. Recommendations were prioritized on a risk-based approach.

All **application vulnerabilities** were addressed by secure coding practices and implementation of strict password criteria in line with St. Michael's Hospital security policies. As an additional measure, CanROC staff run a code scanning software to check any changes to the code prior to live implementation.

High priority **infrastructure vulnerabilities** have been addressed by updates and reconfiguration to web and database servers. A plan is in place for lower risk/priority vulnerabilities that require longer-term implementation plans; in many cases, infrastructure is linked to clinical applications at St. Michael's Hospital and dependencies must be addressed first. For these recommendations that have yet to be addressed, an implementation plan is in effect, and the Deputy Chief Information Officer and Senior Technical Security Specialist at St. Michael's Hospital have approved CanROC operations in the interim considering alternative mitigating measures.

Incidental vulnerabilities have been addressed through the adoption and revision of several Standard Operating Procedures. These SOPs ensure appropriate control, training, and documentation related to CanROC systems are maintained as per industry and institutional standards. Implementation plans for lower risk vulnerabilities are in place, including broader governance documents such as formal business continuity and programming standard guides.

PRIVACY IMPACT ASSESSMENT

The Privacy Impact Assessment (PIA) is an important measure for protecting not only CanROC's patients, but its participating organizations and collaborators. The PIA takes into consideration municipal, provincial, and federal privacy regulations, as well as industry standards and best practice. The ultimate goal is to evaluate risks and provide actionable recommendations.

The analyses conducted included identification and review of key stakeholders, data flows, system operations (including relevant TRA findings), and policies and procedures. Methodology included a combination of documentation review, interviews, and team meetings. The PIA identified 11 probable risk areas with suggested mitigating actions. A summary of the potential risks follows.

As a result of the assessment, the Data Access Committee was established, three SOPs were created, PIA recommendations are informing data sharing agreement language, and the CanROC website has been updated to include details on our governance, information practices, and TRA/PIA findings.

Failure to follow TRA recommendations

If recommendations from the Threat Risk Assessment are not followed, and a breach occurs as a result of not correcting vulnerabilities identified in the TRA, privacy and reputation risk is created.

1. Follow the recommendations of the TRA.

Unauthorized use of registry data

If a study has end points or purposes that are not consistent with the purposes of the original registry study, then the data may not be used for that purpose without new REB approval or DSAs.

1. Implement a data access committee with senior privacy representative from St. Michael's Hospital, CanROC Investigators, and at least one community or lay member.
2. The Data Access Committee will ensure requests for use of study data are allowable within the terms of existing DSAs and REB approval in addition to ethical oversight.

Inappropriate use or disclosure for secondary research purposes

Data collected for specified purposes but without consent shall be used for pulses that allowed collection without consent only. An SOP should exist to verify that a process is in place to handle requests for access to data.

1. Develop and implement an SOP to guide the Data Access Committee.

Unauthorized collection of personal health information (PHI) by abstractors

Not all patient charts reviewed may qualify for entry in CanROC Registry, but all ACRs contain PHI. If research data abstractors are not agents of the Health Information Custodian (HIC) providing the data, viewing ACRs may be considered unauthorized collection of PHI.

1. Obtain clear statement from Disclosing Party (HIC) that the data provided for the study has been collected lawfully and that they assert that they have the authority to disclose this data to CanROC for the purpose of CanROC Registry or related studies.
2. Add a schedule to any data sharing agreement (DSA) with an agency that will be entered into between any abstractor that is not already an agent of the HIC.
3. Implement training to ensure that all abstractors are trained on the appropriate data and tools used by CanROC.
4. Implement SOPs to ensure that incoming records are only handled by individuals authorized to see HIC data, and that patient charts are handled, returned, or destroyed as required.

Unclear demarcation of privacy accountability between CanROC and St. Michael's Hospital

Privacy errors or breaches at Rescu could lead to regulatory or civil actions directed at St. Michael's Hospital, which houses the CanROC dataset, with possible monetary or reputational damage. A formal accountability relationship should be established and documented in data sharing agreements with Health Information Custodians participating in CanROC.

1. Create and implement a Privacy Accountability SOP that delineates roles and responsibly for privacy compliance between St. Michael's Hospital and the CanROC research program.
2. The SOP should consider third party agreements and ensuring adequate training and safeguards at receiving parties, provisions for monitoring and audit, and assurance around destruction of data.

Purposes for collection not properly identified

While the CanROC Registry study protocol identifies objectives of the study, the bases for the collection of information are data sharing agreements; DSAs should provide sufficient data to show CanROC has the authority for data collection.

1. Develop data sharing agreements with each site with focus on local health privacy law where there may be particular requirements or restrictions relating to disclosure of health data without consent for research purposes.
2. Ensure language is included in all data sharing agreements to state that responsibility for ensuring disclosure to CanROC is permitted belongs to the site/HIC disclosing the data.
3. Develop and implement an SOP to regularly review the CanROC Registry protocol and data collected to ensure that only analytically useful data for achieving study purposes is collected.

Retention schedule not justified to meet the requirements and/or purpose

Eventually, all study data must be deleted or anonymized permanently after a defined retention period; otherwise the retention of data past its date of utility would violate privacy principles and regulations.

1. Develop a clearly defined retention schedule and disposal policy for research data.

Weak de-identification methods

Data re-identification techniques are sophisticated and an active area of security and academic research. In the absence of a well-tested methodology, naïve data identification creates significance risk of re-identification in the case of a data breach.

1. Engage a biostatistician or consultant or academic versed in de-identification techniques and develop an SOP to guide de-identification.

Insufficient Openness

Openness is an important privacy principle. The CanROC Registry study is collecting, using, and disclosing health information about individuals, and should make information about the registry publicly available.

1. Provide statements on information practices on the CanROC public website.

No mechanism to respond to enquiries or complaints

If enquiries or complaints from patients or their survivors are made with respect to accessing information or CanROC's privacy practices, an ad-hoc response practice may lead to concerns with consistency or compliance to best practices.

1. Create and implement an SOP for replying to enquiries for access or privacy complaints and ensure contact information is publicly available.