April 7 2017

Rescu Epistry Study and Database Risk Assessments

Rescu is a research program that collaborates locally, across the country, and abroad, handling sensitive data across a range of complex relationships between academic institutions, hospitals, and emergency services. Due to these complexities, the Rescu research team and St. Michael's Hospital, which houses the Rescu Epistry database, underwent an external privacy and security in 2016-2017.

THREAT RISK ASSESSMENT

The Threat Risk Assessment (TRA) is a critical exercise for ensuring protection of electronic data for all Rescu 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 Rescu system to be "Average" compared to similar organizations and systems, and provided recommendations related to three major risk categories:

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

After receiving the TRA report, the Rescu 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, Rescu 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 Rescu operations in the interim considering alternative mitigating measures.

Incidental vulnerabilities have been addressed through the adoption and revision of several Standard Operating Procedures (SOPs). These SOPs ensure appropriate control, training, and documentation related to Rescu 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 patients enrolled in Rescu Epistry, but Rescu's participating organizations and collaborators. The PIA takes into consideration municipal and provincial 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 12 probable risk areas with suggested mitigating actions. It is important to note that a risk does not mean an incident has occurred, or that it is likely occur. Identification of a risk simply means the team should be aware of the possibility of an event negatively impacting Rescu, its study patients, or collaborators.

1. **Unauthorized collection of PHI by data abstractors**
    - Such as viewing of patient charts by research staff without appropriate authority.
2. **Data leakage from Rescu Epistry to associated studies**
    - Such as transferring data to another registry without authorization
3. **Unauthorized use of registry data**
    - Such as releasing data for a publication not aligned with the REB-approved protocol
4. **Unclear demarcation of privacy accountability between Rescu and St. Michael's Hospital**
    - Such as lack of documented accountability between privacy roles of Rescu and St. Michael's Hospital in relation to the Rescu Epistry study
5. **Purposes for collection of data not properly defined**
    - Such as collecting data without the purpose clearly defined in data sharing agreements with the Health Information Custodian providing the data
6. **No provision for the withdrawal of waived consent**
    - Such as a request by a patient to withdraw data, and no procedure in place to do so
7. **Inappropriate use or disclosure for secondary research purposes**
    - Such as sharing data external to the study team without consent, and for a purpose that is not aligned with the REB-approved protocol
8. **Unjustified retention schedule for retaining data**
    - Such as lack of defined retention period of data, or retaining data for a time period beyond when it is useful for fulfilling study objectives
9. **Failing to follow TRA recommendations**
    - Such as failure to apply recommended security controls that leads to a privacy breach
10. **Weak de-identification**
    - Such as failure to apply sufficiently sophisticated de-identification techniques to data releases, such that there is a chance individual patients may be re-identified
11. **Insufficient openness**
    - Such as lack of transparency about the Rescu Epistry study or information practices
12. **No mechanism to respond to enquiries or complaints**
    - Such as request by a patient for information, an no procedure in place to respond

As a result of the assessment, the Data Access Committee was established, five SOPs were updated or created, and the Rescu website has been updated to include details on our governance, information practices, and TRA/PIA findings. Implementation of further recommendations, such as contents of data sharing agreements and additional SOPs, are ongoing.