Threat and Risk Assessment Summary

Enhanced Access to Primary Care - Proof of Concept (POC) – Think Research VirtualCare™

***Date**: July 30, 2019*

Introduction

OTN understands that primary care related solutions must operate in a secure and reliable manner whereby sensitive patient information is protected from unauthorized disclosure, modification and destruction. This report summarizes the security due-diligence efforts conducted by OTN and the Think Research Corporation[1] with regards to the rollout of the Virtual Primary Care solution (Think Research VirtualCare™)[2] for the Enhanced Access to Primary Care POC pilot project. The activities included a formal Threat and Risk Assessment (TRA) conducted by an independent, security consulting company (*Privcurity Consulting*)[3] as well as several security and privacy reviews conducted internally by OTN for new features and enhancements that were introduced following the completion of the TRA.

Project Background

OTN's vision is to provide same-day access to primary care to all patients within a geographic region, whether the patient is affiliated with a family practice or not. OTN has adopted a phased approach beginning with a proof of concept to test and refine the optimal policy, business and clinical model to support scaling of the model to the province. OTN's objective is a scalable, sustainable model of virtual primary care that will spread beyond "early adopter" physicians and patients.

To that end, OTN has established a Vendor of Record arrangement with qualified vendors for primary care virtual visits solutions. Think Research Corporation has been selected to provide a primary care virtual solution Think Research VirtualCare™. OTN has adopted a phased approach beginning with a proof of concept to test and refine the optimal policy, business and clinical model to support scaling of the model to the province. OTN's objective is a scalable, sustainable model of virtual primary care that will spread beyond "early adopter" physicians and patients.

TRA Methodology

The TRA was conducted using the Communications Security Establishment (CSE) and Royal Canadian Mounted Police (RCMP) Harmonized TRA (HTRA) methodology[4] which provides a standard approach for American and Canadian Governments.

Due to the multi-phase/agile nature of the project, several new features were requested by customers and added to the Think Research VirtualCare™ solution after the completion of the TRA. Even though many of these did not introduce significant architectural and/or technological changes to the Think Research platform and were simply extensions of the existing functionality, to ensure that no significant security risks were introduced, each new feature was assessed by OTN's Security and Privacy Teams before being approved for deployment. In cases where severe potential risks were identified, either mitigating requirements were provided or the feature was not given a permission to proceed.

Key Findings

The assessment identified 16 risk scenarios or areas for improvement. Of the risks identified, 10 were rated as MEDIUM and 6 as LOW. These are summarized in the table below:

---

[1] https://www.thinkresearch.com/

[2] https://www.thinkresearch.com/ca/products/virtualcare/

[3] http://privcurity.ca/

[4] RCMP/CSE TRA-1 "Harmonized Threat and Risk Assessment (TRA) Methodology"

Risk 1	Low	Accounts for users that no longer should have access may not be terminated, leaving these individuals with inappropriate access rights.
Risk 2	Medium	Insufficient password policies may result in exposure of patient sessions.
Risk 3	Low	The VirtualCare service offering may not be dedicated (exclusively) to OTN in the future.
Risk 4	Medium	Single-factor authentication and weak password policies may result in exposure of VC patient sessions.
Risk 5	Medium	Inadequate defense in depth design may make it easier to attackers to gain unauthorized access to patient data.
Risk 6	Low	Limited logical and physical architecture documentation and security testing of a relatively new product offering could mean there are unknown vulnerabilities in the proof of concept deployment architecture that could be leveraged.
Risk 7	Medium	Weak (password) policies for TRC administrators may result in exposure or security breach
Risk 8	Medium	Indefinite retention of eVisit data due to undefined OTN retention policy regarding eVisit data unnecessarily magnifies the extent of any breach of EAPC eVisit repositories
Risk 9	Medium	Default encryption levels provided by IBM may not adequately protect patient PHI from unauthorized access.
Risk 10	Medium	Provider accounts may be set up with inappropriate privileges or be set up for inappropriate parties.
Risk 11	Medium	Patient ability to change health history attributes in eVisit patient profile could result in different information between EMR and eVisit.
Risk 12	Medium	Users may upload malware infected files which could then subsequently infect subsequent user workstations.
Risk 13	Low	Limited information does not provide a comprehensive security description of the service offering which may have unknown vulnerabilities that could be exploited.
Risk 14	Medium	Abuse of privilege by IBM and/or solution administrators could result in exposure of patient data.
Risk 15	Low	Limited information regarding PostFix handling of outbound email requests could result in exposure of generated emails. Email push notification traverse through US boundaries.
Risk 16	Low	TRC may not be able to meet OTN availability requirements.

To mitigate these risks and the corresponding vulnerabilities to an acceptable level (Low or Very Low), the TRA provided a comprehensive set of mitigation strategies. While most of the recommendations were immediately applicable to the pilot phase and promptly implemented, some were more practical and suitable in the longer term, should the project go past the Proof of Concept stage and expand provincially. These are summarized in the following section.

Recommendations and Risk Treatment Status

To ensure that patient and customer data is not exposed to undue risk resulting in unauthorized disclosure, modification or destruction of sensitive information, OTN and Think Research have implemented several of the TRA recommendations before the launch or during the course of the pilot. As of the date of this report, the following safeguards have been implemented:

- Procedures for user access reviews have been established.
- Procedures for timely user account deletions have been implemented.
- Stronger password complexity rules have been put in place.
- More strict account lockout thresholds have been introduced.
- Dynamic Web Application Scan has been performed with no High or Critical flaws discovered.
- Additional architectural diagrams have been provided and reviewed.
- Filetype white listing has been implemented to minimize the likelihood of malware being uploaded.
- The PostMark US based email service has been replaced with a Canadian hosted solution.
- High availability architecture has been introduced to satisfy OTN's availability requirements.
- Firewall rules have been implemented to provide logical separation between servers.
- VirtualCare Disaster Recovery Plans and Procedures have been developed.
- Integration with an EMR system has been removed from the scope of the POC.

In addition to the above, the following longer-term recommendations will be implemented should the project go past the Proof of Concept stage and expand provincially:

- 2 Factor Authentication in place for VirtualCare™ Administrators.
- Integration of the VirtualCare™ solution with an anti-virus engine.
- Configure IBM Storage so that Think Research manages all encryption keys or implement Database-level encryption.
- As a SaaS provider, Think Research to obtain a SOC II (or equivalent) certification for the VirtualCare™ solution.
- Establishment of specific Data Retention policies and capabilities.

Please contact OTN's Information Security Department should you have any questions:

Information Security - Ontario Telemedicine Network
438 University Avenue, Suite 200, Toronto, ON M5G 2K8
Email: security@otn.ca | Tel: 416-446-4110

Care. Connected.