Security Risk Assessment Summary

Partner Video Portal

Date: November 13, 2019

Introduction

OTN understands that health 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 with regards to the rollout of the Partner Video Portal as part of OTN's Partner Video Project.

Partner Video Project Background

The Partner Video Project (PVP) is a limited enrollment initiative through which health care organizations and providers can trial and help inform the recommended provincial approach that could enable broader use of non-OTN technology in Ontario, while not inadvertently fragmenting or decreasing access to virtual care. This includes requirements for technology standards, accountability agreements, data/reporting, representation on the directory and enabling supports that may be needed (e.g. procurement, privacy and security). Partners are defined as publicly funded organizations such as hospitals as well as private practice physicians (who themselves are a legal entity). Through the Project:

- Providers are remunerated for care delivered via non-OTN video visit technology that meet minimum standards and guidelines;
- Partners will participate in focused demonstration projects to inform development of a provincial framework for the opening of the virtual care marketplace. These may include testing and supporting workflows for patient host site interactions.
- Partner Video will enable as many providers and organizations as possible to easily use virtual care to expand access to care.

The PVP will present options and recommendations, for Ministry of Health (MOH) consideration, to implement a framework designed to accelerate the adoption and utilization of virtual care technologies, within the context of a coordinated provincial approach. Under MOH direction, OTN will leverage its recent experience with several proofs of concept to launch Partner Video in a phased approach. The goals of enabling partners to use the video technologies of their choice are to:

- increase use of virtual care across the health care sector with a focus on video to the home;
- provide the opportunity to use Hospital Information System/Electronic Medical Record (EMR)-integrated video;
- maintain and where possible improve equitable access to care province wide;
- meet regional and hospital-level needs;
- effectively deliver integrated, high-quality care to patients;
- enhance both the patient and provider experience overall; and,
- create efficiencies in how care is delivered with a focus on reducing hallway medicine

Partner Video Portal

OTN has established a data sharing agreement (DSA) with participating organizations (partners) whereby a limited data set will be shared to enable OTN to report key virtual care indicators to the MOH and back to partners for performance benchmarking.

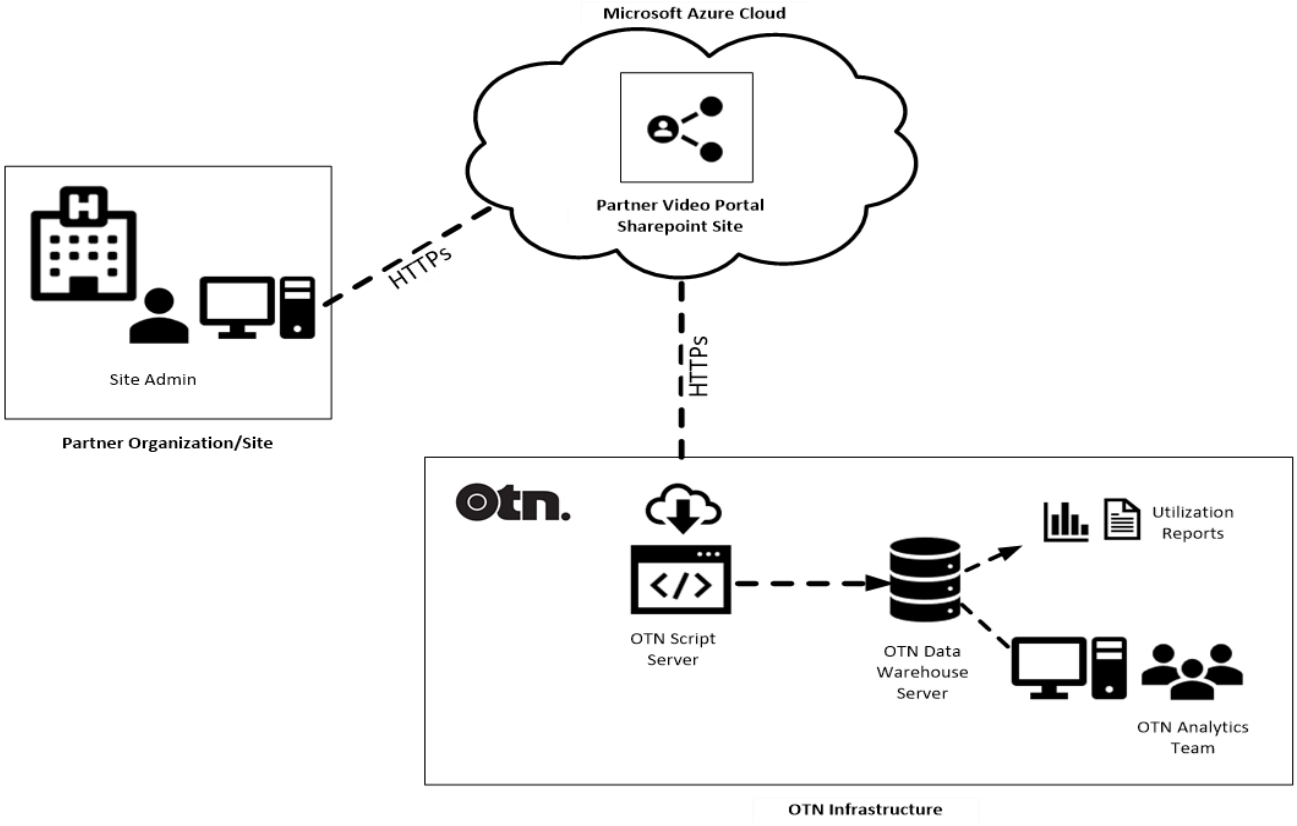
To enable the distribution and collection of the video utilization data, OTN is leveraging Microsoft Azure Cloud and in particular, SharePoint Online as the main technical vehicle. After completing the on-boarding process, obtaining approval and signing the Proof of Concept Agreement, the participating organization will be assigned its own SharePoint portal site. Access to the portal requires an existing Microsoft Office 365 account that is associated with an email address belonging to the organization or the private practitioner.

The portal will host several registration forms (Physician Registration, Program Registration, OHIP Billing Registration), monthly data submission reports, program information, user guides and file transfer scripts. *(Please see the "Asset Analysis" section for more details).*

Participating organizations will be required to submit monthly data reports to the SharePoint portal by the 6th day of each month. The reports are to be submitted as a CSV file and follow the data dictionary specifications outlined in the "**Partner Video Data Specifications**" that is also included on the site.

On the 10th day of the month, OTN's locally hosted Script Server will copy the monthly data report into OTN's Data Warehouse Server, where it will be parsed, analyzed and prepared for reporting by OTN's Metrics Archiving and Reporting System (MARS). Additionally, the script will create an archived version of the file (read-only) on the Partner Video Portal.

The following diagram illustrates the major technical components described above:



Security Risk Assessment Methodology

The assessment of the Partner Video Portal followed a similar methodology and steps as those found in the revised 2006 Harmonized CSE/RCMP TRA Methodology[1] and the NIST Risk Management Guide[2] standards, with some adjustments introduced to account for the unique nature of this project.

In particular, the following workflow was utilized as part of this analysis:

- Determination of Scope
- Information Gathering (Document Reviews, SME Interviews)
- Hands-on Walkthrough (Test Account, Site Demo)
- Asset Analysis
- Threat Analysis
- Vulnerability Analysis
- Risk Assessment
- Recommendations

Scope

In-Scope:

The focus of the assessment was security posture of the SharePoint Partner Video Portal and its intended use to perform the following functions:

- Registration of Physicians/Organizations for the Project
- Registration of Physicians for OHIP
- Submission and sharing of Monthly Utilization Data for Partner Organizations
- Hosting of Project Related Documentation (User Guides, Standards, FAQs, etc.)

[1] RCMP/CSE TRA-1 "Harmonized Threat and Risk Assessment (TRA) Methodology"
[2] NIST SP800-30 "Risk Management Guide for Information Technology"

Out-of-Scope:

The participating organizations and technology providers are responsible for implementing their respective security controls until the upload of the utilization data to the Partner Video Portal takes place. It is at this point that OTN becomes accountable for the security of the submitted data. As such, things that take place prior to this demarcation point are beyond OTN's direct control and therefore were not included in the scope for this assessment.

Furthermore, at the time of the assessment, procedures for onboarding of single practitioners have not yet been finalized. Therefore, this assessment did not consider risks specific to that particular case and was conducted under the assumption that organizational membership is required to participate in this pilot.

Finally, the next phase of the project is considering the use of Power BI for reporting purposes. As no details were yet available, the use of Power BI was also outside of the scope.

Asset Analysis

Confidentiality:

In terms of confidentiality, the most sensitive assets involved within the Partner Video Portal are the **Monthly Data Submission** forms/files. Although individual fields within the file do not disclose personal details about the individual being treated, when combined together (e.g. Participant IP Address, Participant Postal Code, Therapeutic Area of Care, Event Start/End Time, etc.), it starts to create a base from which further information can be inferred. For example, this information could then be combined with data from other sources (e.g. Google Maps, IP lookup, etc.) to possibly identify the individual receiving treatment. This is particularly true in smaller, less populated areas, where the postal code or the IP Address range is shared among fewer individuals. Hence, the **Monthly Data Submission** file is considered Personal Health Information (PHI) and as such has a Confidentiality Rating of **High**.

By extension, since the confidentiality requirements of Passwords and Private Cryptographic Material are at least as great as the data they protect, Partner Video Portal **Password** and **Private Cryptographic Key** used to encrypt the Monthly Data Submission have been assigned a **High** Confidentiality Rating as well.

Integrity:

Although there are no critical clinical or business decisions that depend on the accuracy of a single document within the portal, errors and/or omissions in the registration documents could cause some delays during the on-boarding process, these would be considered minor interruptions and would not have significant impact on the project as a whole.

From the Integrity protection perspective, the most crucial are the two PowerShell scripts, whose source code OTN makes available to the users of the Partner Video Portal. The first of these scripts creates a password file that is to be used for encrypting the Monthly Data Submission file prior to uploading it to the Partner Video Portal. The second script file applies the password generated from the first script and encrypts the Monthly Data Submission file and allows the user to upload the file from a local folder to the Partner Video Portal SharePoint Site. As these scripts are responsible for generating private keys, encrypting and transmitting a file that contains PHI, any tinkering with these scripts could compromise the file's security and/or send to an unintended location. As a result, these PowerShell scripts have been assigned a **High** Integrity Rating.

Availability:

Since **Monthly Data Submission** files are submitted and collected on monthly basis (submitted to the portal on the 6th business day of the month and collected for reporting on the 10th), significant downtime can be tolerated without having severe impact on the project. If for example, the Portal were to become unavailable on the 6th business day of the month, the upload process could then be repeated once the portal is back online. All of the assets involved have been assigned a **LOW** Availability Rating.

Threat Analysis

The overall threat landscape with regards to the Partner Video Portal initiative is **LOW to MEDIUM** which is in proportion to the project of this nature and size.

There is no data or information in the Portal that would be particularly attractive or valuable to external adversaries (one could be quickly sold for profit, personal gain and/or blackmail). As mentioned in the Asset Analysis section, the **Monthly Data Submission** file on its own does not provide much useful information and would have

to be combined with other data sources to identify participating individuals. This would require a significant amount of time and persistence and is an example of a 'high effort and low reward' scenario.

A more likely scenario, with regards to external threats, would be a non-targeted situation, where a hacker accidentally stumbled upon the portal's URL as part of a random scan or reconnaissance activity, in which case it was more likely the Microsoft Azure Cloud that was targeted and not the Partner Video Portal.

The most relevant and applicable threats, with regards to the Partner Video Portal are the internal users who have already been provided access to the portal. In this case, the cause of the threat could be accidental (inattention to instructions, fatigue, lack of training) or deliberate (disgruntled/terminated former employee, curious current employee). Still, the amount of damage potentially inflicted to either OTN or the individuals participating in the project would not be very significant.

Vulnerability Analysis

The analysis of the implemented safeguards as well as the hands-on walkthrough of the Partner Video Portal Demo site revealed a number of security deficiencies/vulnerabilities that could be exploited either deliberately (by a motivated/skilled individual) or accidentally (by a careless or untrained user).

The most significant of the identified vulnerabilities are listed below:

Lack of Control over Password Policy Enforcement – In order to access the Partner Video Portal, users are required to have an existing Microsoft Office 365 Account that is tied to the user's organization email. Although, there are basic password complexity requirements and policies enforced by Microsoft (https://social.technet.microsoft.com/wiki/contents/articles/40140.office-365-password-policy.aspx), some of these can be relaxed based on the organizational policies. As a result OTN has no control over the password policies that are applied when authenticating to the Partner Video Portal.

Lack of Multifactor/2-Step Authentication – Currently, only a username and a password are required to log into the Partner Video Portal. With internet facing systems, particularly those hosting confidential information, it is a security best practice to use a 2 Factor Authentication (password + something the user has/or is)

or 2-Step Authentication where a one-time-password is sent to the user's phone or email.

Lack of Filetype Validation/Whitelisting – Although it is expected that registration information and data submission files will be submitted using the provided CSV and PDF sample files, there is nothing restricting users from uploading other kinds of files, including Microsoft Office files with embedded Macro scripts. Although, SharePoint Online scans files for viruses (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/virus-detection-in-spo) , it is not intended as a single point of defense against malware. Limiting the upload of files to only those that are required (CSV) would provide an additional layer of protections against malware and malicious script.

Read/Write Access Permissions to PowerShell Scripts – Currently, the portal provides each site's admin a read/write access to PowerShell Scripts that were prepared by OTN's IT Administrator to generate a private key, encrypt the Monthly Data Submission file, and enable a scheduled automated upload of the file to the Partner Video Portal. The site admins are able to modify the script files as they wish which may result in the security of the file (encryption) being compromised or the site credentials being revealed if modifications to the file are not applied diligently.

Current version of MARS has not been subjected to a Security Review – Hosted locally behind OTN's Network Perimeter (not exposed to Internet) and protected by OTN's network security safeguards, OTN's MARS server is sufficiently protected from external (public) threats. However, the system has not been recently subjected to a detailed Security Review and may contain deficiencies leading to misuse from internal users.

Risk Assessment

The aggregate risk to OTN and the Partner Video Portal is **MEDIUM** bordering on **LOW**. The risks that were identified as part of this assessment are listed in the table below along with applicable recommendations. As this is a pilot/proof of concept project, it is important to note that the risk ratings may change as new functionalities or processes are introduced and the project is introduced to a larger group of participants.

Risk	Original Risk Rating	Recommendations	Status (as of Nov 13, 2019)
Risk1: Unauthorized Access to the Partner Video Portal.	**MEDIUM**	Enable 2-Step Authentication in which case a site admin will be required to enter a One-Time-Password (sent to their organizational email address) in addition to the regular username/password.	**Accepted** (for the POC Phase)***** ****Note:*** *Enabling 2-Step Authentication at this stage, would disable the automated report transmission functionality. OTN will explore 2-Step Authentication as part of future phases.*
		The Proof of Concept Agreement, should require participating organizations to notify OTN when a site administrator is no longer with the organization, so that access can be revoked in timely manner.	**Completed**
Risk2: Exposure of Confidential Information contained in the Monthly Data Submission file resulting from modification of the Encryption/File Transfer PowerShell Scripts.	**LOW**	Implement Role-Based Access Controls to ensure access to scripts is granted on a "Need to Know" basis.	**Completed**
		Minimize the likelihood of scripting errors by providing users with a written set of instructions regarding the scripts' usage.	**In Progress**
Risk3: Partner Video Portal being used to host malicious scripts, malware or "garbage" data.	**LOW**	Enforce Filetype Validation/Whitelisting, so that only expected filetypes and formats are allowed to be submitted.	**In Progress**
Risk4: PHI Data submitted to MARS may not be sufficiently protected from internal threats.	**LOW**	Perform Security Assessment/Review of OTN's MARS system.	**In Progress**