# Ontario Health (OTN) Services and Safeguards
# Vivify Solutions

## Description of Services

Ontario Health (OTN) (OH) is an independent, not-for-profit organization funded by the Ontario Ministry of Health. Using advanced information communication technologies and electronic medical devices, OH supports the delivery of clinical care, professional education, and health-related administrative services at more than 1,600 urban and rural sites across the province.

OH, is committed to protecting personal health information consistent with the requirements of the '*Personal Health Information Protection Act,* 2004' (PHIPA) and Ontario Regulation 329/04. "Personal Health Information (PHI)" is any information that can identify an individual and relates to their health care services received. This includes but is not limited to name, address, telephone number, health card number, health care provider's name, the reason one was referred for a telemedicine appointment and any examination results.

OTN's Telehomecare program allows individuals to enjoy the best possible health while staying in their own home if suffering from Chronic Obstructive Pulmonary Disease (COPD) or Congestive Heart Failure (CHF). Telehomecare is available in most, but not all areas of the province. Easy-to-use equipment and health coaching by a Telehomecare clinician can help manage conditions at home.

Telehomecare provides families and volunteer caregivers with the assurance that their loved one is closely monitored and, at the same time, learning how to make the best lifestyle choices to keep them as healthy as possible.

Telehomecare is a chronic disease management intervention for individuals living with chronic illness (COPD and /or CHF), supported by remote monitoring technology in home. Individuals are referred into the program by any member of their care team and should expect to be enrolled for approximately 6 months. Telehomecare Clinicians work with their patient's Most Responsible Provider (MRP) and relevant Healthcare Team to ensure continuity and consistency of their care. Provided by host organizations across the province and delivered by a registered health care provider with specialized training in health coaching and self-management support.

## How the Technology Works

OH, brings virtual care innovation to the healthcare system so that the people of Ontario can get the care they need when and where they need it most: at home, in their community or in hospital. For more than a decade,

OH has increased access to health care and education across the province with one of the world's most extensive telemedicine networks. Working with its many partners and leveraging its unique knowledge of health care and digital technology, OH addresses challenges by introducing and spreading new ways of delivering care that benefit patients, care providers and the healthcare system.

OH engaged Vivify Health to develop, host and administer the Telehomecare's (THC) Patient Monitoring and Management System (PMMS). The Vivify solution that is currently deployed has 2 modalities of access for patients:

- Fully managed kits consisting of an Android tablet and health monitoring devices such as blood pressure cuffs, pulse oximeters and/or weight scales. These Bluetooth enabled devices are paired with the tablet by Vivify Health allowing the app on the tablet to automatically obtain the device readings and upload them to Vivify. The entire kit is pre-configured by Vivify and shipped to the patient as part of enrolment; and
- A BYOD (Bring Your Own Device) solution where the patient uses their own health monitoring devices and uses a mobile web browser app to manually enter their device readings and upload them to Vivify.

Vivify has released a mobile app (Vivify GO+ v2.0 for iOS and Android) as a new feature of their service on May 30, 2019. These apps provide features to patients wanting to use their own health monitoring devices through the current BYOD browser solution, including:

- Bluetooth connectivity to a list of Vivify-supported health monitoring devices;
- Biometric Self Trending on patient's smartphone;
- Secure Messaging between the patient and their Patient Care Team;
- Video visits between the patient and their Patient Care Team; and
- Educational Videos and Health Tips.

OH would like to make these apps available for patients with their own monitoring devices attending delivery sites who are using remote monitoring services from Vivify. Using these apps as an alternative to the current BYOD solution will provide these patients capabilities similar to the Fully Managed Kit solution.

New SMS enhanced functionality will be enabled that was outside the scope of the original PIA assessment and as such an internal Statement of Risk was conducted on *November 19, 2019.*

While the Vivify Remote Patient Monitoring solution is hosted in Ontario and data associated with this component of the solution (provider station and patient tablet) remains in Ontario, it was identified that the Vivify Go (Mobile Apps) solution stores and transmits some personal health information outside of Canada i.e.: **The patient mobile number, and any configurable messages to the patient would be transmitted and stored in the United States of America through an application programming interface (API) to Vivify's for Short Message Service (SMS) provider Twilio.**

The Virtual Healthcare Program team proposes the Cloud Computing Services, Use and Procurement and Third-Party Services Provider policy acceptance of a limited amount of personal health information being sent outside of Canada to allow patients to have the option of how they wish to receive notifications. One of the learnings

from the BYOD pilot was that patients would prefer their notifications be delivered via SMS, not email. Vivify Go+ sends the invitation to the patient via SMS from the care team portal with a link to the Apple store or Google Play Store to download the application. Additionally, as part of the authentication process the Care Team Portal sends a PIN to the patient via SMS. **The patient retains the option of using email and/or SMS.**

Personal Health Information (PHI) is not stored on the patient's device. PHI is in transit after the patient enters the information on their phone, and then it is securely stored in the Care Team Portal databases. Information that is stored on the phone is related to the settings the patient chooses, such as "Remember Me" and "Stay Logged In."

After a patient is created in the Care Team Portal, they will be sent an invitation text message and/or email, so they can download the +Go app to their smartphone or access the site from their device's browser. Patients are assigned a PIN number by the system, which is used for authentication.

## Privacy and Security

OH, follows industry best practices (e.g. ISO security standards) and legislative requirements (e.g. PHIPA). The Privacy and Information Security teams play an active role in building and managing privacy and security within OH products and services. Only those OH employees with a business "need to know" and whose work duties reasonably require it are granted access to personal and personal health information.

OH, has a comprehensive privacy program in place that addresses the privacy rights of patients in accordance with PHIPA. As a Health Information Network Provider (HINP), Service Provider and Agent under PHIPA and its regulation, OH provides comprehensive services to its members and users, including health information custodians (HICs) and non-custodians, to support them in meeting their obligations and responsibilities under PHIPA and other applicable privacy legislation.

- For this engagement compliance with PHIPA is a shared accountability between OH and Vivify.
- For this initiative, OH will be acting as an Electronic Service Provider (ESP) pursuant to section 6(1) of O.Reg. 329/04. Vivify is a Third-Party Service Provider to OH when it receives, stores, uses and transmits PHI between the patients and the Host Hospitals.
- OH as an Electronic Service Provider (ESP) does not collect, use and disclose PHI when providing services (through its 3rd party service provider Vivify) pursuant to section 6(4) of O.Reg. 329/04.
- The Host Hospital (HIC) is the custodian of the PHI transmitted via the iOS and Android +GO apps and +GO Web app.
- Both OH and Vivify have comprehensive privacy programs in place that address the privacy rights of patients in accordance with PHIPA and Ontario Regulation 329-04.

## Privacy Governance at OH

OH, has established a comprehensive privacy governance structure and has full time, dedicated privacy employees to address privacy and information management requirements and issues.

## Description of Safeguards

OH monitors, reviews and updates its practices to ensure the privacy and security of confidential information (including PHI and PI), processed on its systems and transmitted over its network are safe and secure. OH, uses a variety of physical, administrative, and technological safeguards to protect confidential information from unauthorized access, use, copying, modification or disclosure *including contractual agreements* with all of its members. The safeguards described below are not meant to be an exhaustive list and are not limited to:

### OH Administrative Safeguards

- OH, has entered into a Master Agreement (MA) contract with Vivify that detail privacy and security related requirements, obligations, roles and responsibilities. OH, relies on such an agreement and the accompanying Statement of Work (SoW) with Vivify to build, operate and define deliverables and accountabilities for the end-to-end privacy and security of the Vivify solution.
- A Privacy Impact Assessment (PIA) and Threat and Risk Assessment (TRA) and a Statement of Risk on the SMS functionality have been conducted concurrently to identify, assess, and mitigate privacy and security risk for the Vivify initiative. The TRA and PIA and Statement of Risk should be considered companion documents in providing a comprehensive overview of safeguards.
- Privacy and Security policies and procedures are in place as set out in frameworks.
- Employees receive mandatory privacy and security training upon hire.
- Employees sign an Employment Agreement and Confidentiality Agreement.
- Staff with access to PHI are required to undergo Criminal Background Checks.
- There are dedicated full-time Privacy and Security employees to lead the assurance and compliance efforts.
- Roles & Responsibilities of Members and Participating Organizations are provided in Terms of Service Agreements.
- OH, has established procedures to address policy violations by employees.
- OH, has audit log that log every access, modification, or disclosure of PHI, together with the time and identity of the accessing user.
- OH, routinely monitor audit logs for unauthorized access to PHI by staff.
- OH, has implemented policies and procedures to manage privacy and security incidents and breaches.

### Technical Safeguards

OH's overall quality assurance process includes detailed security testing. This testing not only includes validation that components and services are operational, and that key security safeguards are implemented and operated to the necessary degree to minimize the organization's exposures. OH, also recognizes that testing is vital not only to maintain security controls but to reduce the organization's risk profile.

### Vivify Administrative Safeguards

- Internal security audits and assessments are conducted regularly
- Management approved Risk Management Plan and Risk Management Polices & Procedures are in place
- Comprehensive set of Security policies aligned with HIPAA Rules

- Robust Governance Structure In Place; Information Security Management, Co-ordination, and Allocation of Responsibilities
- Attained Canada Health Infoway Certification; March 2018
- Internal audit of implemented security controls based on HIPAA Rules has been conducted
- HIPAA Security Rules are enforced in all IT procurement contracts
- Information classification and rating of IT assets is in place
- All Staff are required to complete Health Insurance Portability and Accountability Act (HIPAA) training and Privacy & Security training annually
- Mandates change controls process be established with requirements along with testing of any changes introduced in the production environment.
- Segregation of duties for change management and implementing changes is in place
- Complete acceptance criteria for acquired/developed/upgrade software is in place
- Regular testing of system security controls takes place regularly
- End User License Agreement
- Inactive accounts are automatically disabled after a period of 90 days
- User accounts audited by Vivify Health Security Analyst
- Vulnerability management and penetration testing are being performed as required
- Systems are regularly monitored for vulnerabilities and patched accordingly
- Secure Software Development Life Cycle is in place that involves
    - SCRUM Agile process for development and testing
    - JIRA to track defects as well as releases
    - Secure coding practices + Input Validation
    - Heed compiler warnings
    - Secure Architecture design
    - Default deny
    - Adherence to the principle of least privilege
    - Sanitization of data
    - Use effective quality assurance techniques (fuzz testing, pen test and source code audits)
- All releases subjected to QA test cases prior to promotion to production

## Physical Safeguards

- 2 Ontario Data Centres are ISO 27001:2013 and ISO 9001: 2008 Compliant (Alcumus ISOQAR)
- York Street Data Centre (backup for Vivify) is both ISO and SOC II compliant
- Infrastructure as a Service (IaaS) services are provided by CentriLogic in Mississauga which is HIPPA-HITRUST, PCI DSS, ISO27001, SSAE126 and Privacy Shield Framework certified
- CentriLogic as an IaaS provider is responsible for network layer security and physical level security per the contract stipulations.
- Multiple Utility Power Feeds
- Backup Generators
- Redundant UPS Systems
- Strict Climate Controls
- 24/7 Monitoring & Management
- Fire Detection & Suppression

## Technical Safeguards

- Technological separation of development, testing and production environments is enforced

- Backups are stored on disk in the primary Data Centre and replicated to backup Data Centre across WAN. Data is encrypted using VPN across WAN
- Backup alerts and notification regarding the status of backups and replication activity
- Multiple Bandwidth Partners & Peers
- Use of cryptographic controls and protection of cryptographic keys
- Uses SSL/TLS protocol to authenticate sessions and secure transmissions 256 bit TLS 1.2
- Encrypted Data at Rest and in transit
- All connection to 3rd Party Services uses SSL - only email is clear text
- High-Speed Inter-facility Connectivity
- SQL Server 2016 R2 database is encrypted using AES 256 Transparent DB Encryption
- Maintains system auditing (configuration history, system logging/faults)
- Each login captures caregiver id, session token, IP address, time/date and user agent (browser)
- Verify IDS/IPS, SIEM, log review, capacity mgt in place from PaaS
- Logs stored in SQL Table. Database encrypted
- Access controls are in place to prevent unauthorized changes
- All servers time synchronized using Windows server time synchronization

***Where can I get more information about OH's or Vivify's Privacy Practices?***

Please contact the Privacy Office should you have any questions:

***Ontario Health (OTN)***
***438 University Avenue, Suite 200, Toronto, ON M5G 2K8***
Email: privacy@otn.ca | Tel: 416-446-4110 / 1-855-654-0888 / TTY: 1-855-368-6889