Care. Connected.

Privacy & Telehomecare

Ontario Telemedicine Network (OTN) - Privacy and Risk Office
Email: privacy@otn.ca | Tel: 416-446-4110 / 1-855-654-0888 /
TTY: 1-855-368-6889

Private & Confidential 2018/2019

Objectives
At the end of this learning session you should:

1. Understand the relationship between OTN & your Organization as it relates to Telehomecare
2. Have awareness of OTN's privacy due diligence efforts
3. Recognize your privacy related roles & responsibilities in using new software from Vivify Health Canada Inc. ("Vivify")
4. Understand the importance of privacy when using Vivify to support your Telehomecare patients
5. Identify key requirements to ensure privacy in healthcare when using mobile & portable devices
6. Harness the power of social media & minimize risk as it relates to Telehomecare
7. Recognize & report privacy incidents/breaches in a Telehomecare environment

OTN Telehomecare & Your Organization

1. OTN is a world leader in telemedicine helping Ontarians get the care they need, where and when they need it; at home, in their community or in hospital.
2. The OTN Telehomecare Provincial Program supports patients with chronic obstructive pulmonary disease (COPD) or congestive heart failure (CHF), plus diabetes as a comorbidity, through health coaching and remote monitoring.
3. OTN provides Telehomecare to your Organization using a Third-Party Cloud Software as a Service platform (SaaS) from Vivify Health Canada, Inc. ("Vivify").

Privacy Is A Joint Responsibility

1. Privacy is a joint responsibility between OTN, your Organization, Vivify Health Canada, Inc. and You.
2. We are building a provincial reference model for Telehomecare…we want to lead by example.
3. Healthcare Providers expect privacy & patients deserve it…it's their right and will ultimately depend on the people working in Telehomecare.
4. Ensure you have the tools and services in a manner that enables you and your Organization to meet your privacy requirements and be successful.

OTN Privacy Due Diligence

OTN's Privacy and Risk Team undertook a number of due diligence exercises in collaboration with the Team that procured Vivify. Governed by OTN Privacy Policy Framework; below are some of the controls, policies and best practices that were leveraged:

1. Cloud Computing Services Use and Procurement
2. Privacy Impact Assessment
3. Privacy Training and Awareness
4. Retention, Transfer and Destruction of Confidential Information
5. Limiting Agent Access to and Use of Personal Health Information, Privacy Audits and Monitoring
6. Privacy Breach Management
7. Executed Master Services Agreement with Vivify
8. Updated OTNhub Terms of Service Agreement

OTN Privacy Due Diligence

1. Re-freshed Privacy and Security training for OTN Members
2. Re-freshed Telehomecare Patient Brochure/Pamphlet
3. Conducted a Privacy Impact Assessment (PIA) with respect to threats, vulnerabilities and risks to the security and integrity of PHI and a Threat Risk Assessment (TRA)
4. Performed detailed Quality Assurance and Security testing prior to making Vivify software available
5. Vivify procurement & program launch executed via OTN Gating Methodology

What You Should Know When Using Vivify

1. When accessing Vivify, please be aware of your physical surroundings and protect patient confidentiality by being mindful of physical surroundings and audiences when discussing their conditions i.e coffee shops.
2. Only log-in from secure connections i.e. https
3. Participate in future Vivify and Telehomecare training opportunities as they become available
4. Visit OTN’s Telehomecare Center regularly for updates and new best practices
5. Patients can also self-refer on OTN’s website, by going to https://ontariotelehomecare.ca and using the postal code sorter to find contact information for the Telehomecare program in their region

What You Should Know When Using Vivify

6. You have been provisioned with a role in Vivify (Clinician, Nurse, or Manager) that aligns with your access to personal health information. If it needs to change, please notify OTN at the earliest opportunity; eCareSupport@otn.ca.
7. If you no longer need access to Vivify, please notify OTN at the earliest opportunity; eCareSupport@otn.ca.
8. Always report privacy incidents/issues/breaches to your Privacy Officer and privacy@otn.ca.

Working in Telehomecare using tools in a digital and mobile environment

Remember to always follow your Organization's policies & procedures

The following are OTN recommended best practices with respect to protecting privacy in mobile healthcare environments

Mobile Privacy In Healthcare Environment

1. Changes are that you use mobile devices when you are at work, at your home office, in transit while travelling for work or while conducting home visits.
2. Security for mobile devices is twofold. Ontario’s Information and Privacy Commissioner expects strong end-to-end encryption of data **and** the use of strong password protection
    1. Use an uppercase and lowercase letters, numbers and special characters (e.g. Hello6Bonjour%)
3. Change passwords with access to confidential information (e.g. PHI) as per your Organization’s policies.
4. Sensitive data should not be:
    1. Stored in a laptop, tablet, USB key, or personal folder.
    2. Accessed or transmitted via public wireless networks, which are by nature open and therefore not secure.

Mobile Privacy In Healthcare Environment

5. Ensure that configuration of your mobile device allows for remote wiping of data in the event it is lost/stolen.
6. Comply with your Organization's policies and requirements regarding communicating with patients via email, text or wireless media.
7. Know and follow your Organization's procedure for reporting incidents.
8. Be aware of eavesdropping, or someone looking over your shoulder "shoulder surfing" in public areas.
9. Avoid usage of PIN-to-PIN messaging for sharing sensitive data; information transmitted this way is highly insecure and easily intercepted.

When Mobile Devices Are Lost or Stolen

1. Be prepared ahead of time to respond effectively will ensure the least damage to personal health/personal information.
2. Know and follow your Organization's procedure for lost or stolen devices.
3. If you suspect a mobile device has been lost, stolen, inappropriatelyaccessed or otherwise compromised:
   1. Notify your Privacy or Security Officer so they can remotely wipe the device
   2. Notify patients as required
   3. Notify the IPC in accordance with your Organizational policies
   4. Contact OTN (privacy@otn.ca)

To Summarize / Key Considerations

1. Prevention is key, but incidents happen.
2. Patients trust you to protect their PHI and as a user, you bear responsibility; be proactive.
3. Ask your Privacy and Security Officers to assist you in enabling the best privacy and security controls available.
4. Use discretion in selecting the best process/tool for sharing personal health information for any particular purpose.

Social Media

Harness Power Of Social Media

1. OTN promotes and supports responsible and effective use of social media
2. Harness the power of social media & minimize risk as it relates to Telehomecare
3. Social media provides new tools to break down barriers in the health care discourse among patients, providers and organizations
4. Responsible and effective use of social media enables:
    1. The open exchange of ideas, best practices & quality improvement opportunities
    2. Better collaboration across health disciplines, resulting in better informed health care delivery for the patient
    3. Increased tools available to facilitate learning opportunities & finding colleagues with shared interests

Key Challenges

Social networking tools, such as Facebook, Twitter, LinkedIn, Blogs, Podcasts, YouTube, Wikis and online discussion forums are blurring the line between traditional notions of “public” and “private”

Information posted to your personal social media accounts may be accessed by employers (current and prospective), insurance companies, colleagues, patients and others

Information posted on social media pages is subject to requests for discovery in legal proceedings, whether an individual has clearly identified themselves or posted anonymously

Information, once posted in a social media forum, may be difficult to modify or permanently delete. Think twice before posting as is likely to remain there forever

Across the spectrum of social media, there exists a real “mixed bag” of policies, privacy and access controls, risks and benefits to consider

Users must conform to guidelines for usage – do not own the content

Key Challenges

Site owners can retain authority to use, manage, share, edit or remove content without your authorization

Online data constantly mined, cached & reposted = retrieval difficult or impossible

Information mined can be sold to third parties with commercial interest in such data

Google search history is mined & sold to advertisers and marketing firms

Developers of Twitter apps can access people's private messages

Postings to public blogs & discussion forums can be crawled by search engines and may appear in search results

Profile aggregators crawl & mine information & build directories of individual/public profiles (connecting personal & professional information). For fun, search yourself

No guarantee of privacy and many unseen listeners

Use of Social Media in Health Care

1. Never share personal health information….ever!
2. Ensure online discussions do not include details that could identify a specific individual
3. De-identifying means more than removing a patient’s name. i.e redacting date of birth, home address, personal email
4. When discussing a specific patient with another care provider use secure communication tools, not social networking sites
5. Do not discuss in a virtual public forum anything that you wouldn’t discuss in a face-to-face public forum
6. Don’t connect with or accept patients/clients or former patients/clients as ‘friends’ on social media sites - could be at risk of breaching therapeutic relationships

Use of Social Media in Health Care

7. Never disclose confidential, sensitive or individually identifying patient information or personal information via social networking sites
8. Always be aware of the possible impact of social media, whether used in your personal or professional sphere
9. Remember that your current standards of practice still apply when utilizing social media/networking
10. When posting to any social networking site, whether personal or professional in nature, assume that information is out there for all to see
11. Be mindful of how much information you share on social media as is susceptible to being collected and used to steal your identity
12. Exercise discretion – once posted, information may be difficult to permanently delete or modify

Use of Social Media in Health Care

13. Never post information which could be defamatory or damage the reputation of others, or your organization. For example:
    “*The ICU team leader needed a female bed on our ward…..then brought a different patient who was male… she has no idea about anything, I think they make her leader so she doesn’t hurt anyone!!!*”
14. If speaking on behalf of your organization, follow your organization’s communication/social media policies
15. Social networking sites update their policies regularly, be sure to keep up with the changes and update your profile/account settings frequently

Privacy Incidents

Recognize & Reporting Privacy Incidents/Breaches

1. **What is a privacy breach?** When personal health information (PHI) is lost, stolen, inappropriately accessed, used, disclosed, copied, modified or disposed.
2. Know how to recognize & report privacy breaches in a Telehomecare environment – Examples include the following:
    1. Sending a Telehomecare report outside the Circle of Care
    2. Access to patient information you are not authorized to
    3. Looking up a patient's PHI if not authorized to do so; i.e. Snooping into patient records
    4. Disclosing PHI without consent
    5. Misdirected fax
    6. Email personal health information if unencrypted/inadequate safeguards ***or*** not in compliance with Organizational policies
    7. Storing PHI on unencrypted mobile devices (loss & theft)

Recognize & Reporting Privacy Incidents/Breaches

1. Your role in reporting privacy incidents and breaches:
    1. Report privacy incidents/issues/breaches to your Privacy Officer
    2. Report to OTN's Privacy and Risk Team via privacy@otn.ca

Recognize & Reporting Privacy Incidents/Breaches

How reporting privacy incidents works between your Organization, OTN, and Vivify Health Canada, Inc.

1. At the first opportunity of learning of a potential privacy incident at your Organization, please report to OTN via email; privacy@otn.ca.
2. OTN Privacy Team would then report via email to Vivify Health Canada, Inc. who shall respond and acknowledge within 1 business day (Or sooner).
3. If for any reason, email cannot be reached, OTN Privacy Team will call Vivify Health Support, and report the purpose as “Privacy Incident” or “Security Incident.”
4. Vivify will initiate an incident related ticket and share this with the appointed OTN Privacy & Security Staff within 15 minutes.
5. An Incident Management report by Vivify Health will also be created, updated and shared with OTN Privacy Team during the investigations till closure.
6. Your Organization, Vivify and OTN will work collaboratively throughout the investigation process getting to root cause, and recommendations/improvement opportunities to prevent from future occurrence.

Thank You

For any Telehomecare program related privacy questions, contact your Organization's Privacy Office first; and then OTN's if needed

OTN Privacy and Risk Office –
Ontario Telemedicine Network
https://otn.ca/about-us/contact-us/
Email: privacy@otn.ca