MANAGING PRIVACY

DURING VIRTUAL FAMILY VISITS

A Toolkit for Care Facility Staff

Created by KnowledgeFlow Cybersafety Foundation

In Partnership with Managed Privacy Canada

Our sincere thanks to Adejoke Osuntogun, Keri Horan, Onomo Ogbe, Uche Umeh and Amber Stefan for their valuable contributions.

This project is funded in part by the Government of Canada.

Canada

PURPOSE

As the world continues to adapt to our new reality, in this era of pandemic-related restrictions and social distancing, many residents in care homes have begun to use various virtual platforms to connect with and keep in touch with loved ones.

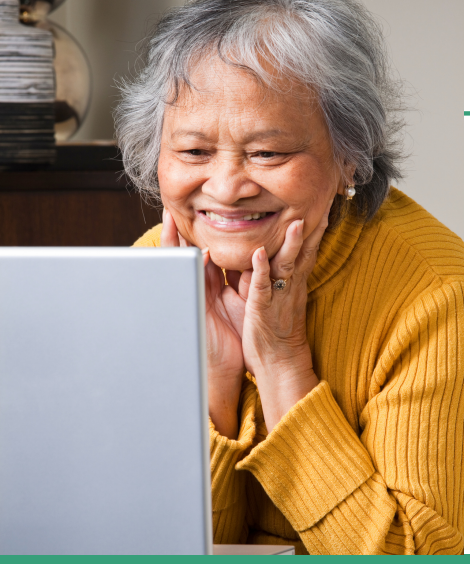
This toolkit explores the unique privacy and security concerns encountered during these virtual visits. It presents practical tools to manage the rapidly evolving privacy threats and mitigate potential losses and misuse of residents' personal information.

No video conferencing software can be considered completely secure.

OVERVIEW OF PRIVACY CONCERNS

Privacy Concerns During Virtual Visits Include:

- Unauthorized/uninvited participation
- Recording of visits (by either party)
- Screenshots / photos (by either party)
- Intrusion into the privacy of other residents
- Unintentional disclosure of sensitive personal information



FAMILY OF RESIDENTS' PERSPECTIVE:

- Family should expressly consent to the collection, use and disclosure of their personal information for the purpose of conducting the virtual visits.
- Family must endeavour to join virtual visits from secure locations.
- Family should also ensure that unauthorized persons do not participate or have access to the virtual sessions.
- Family should not share sensitive information (e.g., financial information and personal health information) during the virtual visits.
- Access to devices used during the virtual sessions containing personal information should be restricted.

Residents' Perspective:

- Residents should be educated & supported in operating the devices and using different features that ensure their privacy during virtual visits (e.g., the use of headphones and background images).
- The organizers must obtain the residents' informed consent on collecting, using and disclosing their personal information before the sessions.
- Residents should be informed of their right to modify or withdraw their consent given on the collection, use and disclosure of their personal information at any given time.
- Residents should be enlightened on the potential risks in sharing sensitive personal information over virtual platforms.

STAFF PERSPECTIVE:

- Staff should receive comprehensive privacy and security training on the collection, use and disclosure of residents' personal information.
- Staff should receive training to use virtual meeting platforms to conduct the visits securely.
- Staff organizing the sessions should commit to respecting their privacy obligations (e.g., confidentiality).
- Staff should receive clear guidelines on which virtual platforms are to be used and what equipment provided by the facility is to be used to conduct the virtual visits.

Staff should be aware of the Residents' Bill Of Rights which is part of the Long-Term Care Homes Act. Available at www.cleo.on.ca

Personal information collected for the purposes of a virtual visit may include: name, phone number and email address

PERSONAL INFORMATION MAY BE ACCIDENTALLY VIEWED OR RECORDED DURING A VIRTUAL VISIT

- files/tabs left open during screen sharing
- audio of non-participants in the background
- people or information viewable in the background of participants

Discussing medical information with family members should be carefully restricted during virtual visits.

Discussing sensitive financial information with family members should be prohibited during virtual visits.

GENERAL BEST PRACTICES:

During Virtual Visits

1. A unique password should be generated for each session.

2. Each session should start with the camera and audio turned off to prevent unintended disclosures.

3. The camera should also be turned off or blocked when not in use.

4. There should be proper identification of all the participants by the organizer before a session commences.

5. The participants must be informed of the types of sensitive information that are not advisable to share over the virtual platform.

6. The participants should be discouraged from recording the session or otherwise storing information shared due to privacy concerns.

7. Participants should be informed if an employee will be participating in or monitoring the session to assist the resident.

BEST PRACTICES

Physical Precautions

1. Servers and devices containing personal health information, such as desktop computers, laptops and tablets, should be kept in a secure location.

2. Security measures like alarm systems should be put in place to restrict access to rooms where equipment and personal data are stored.

3. Staff should restrict the use of any equipment which contains personal information to authorized purposes only.

4. Appropriate measures should be enforced to prevent unauthorized persons from participating in or accessing the virtual sessions.

5. Privacy features like blurred backgrounds and images should be used to prevent accidental viewing of non-participants.

Cybersecurity Precautions

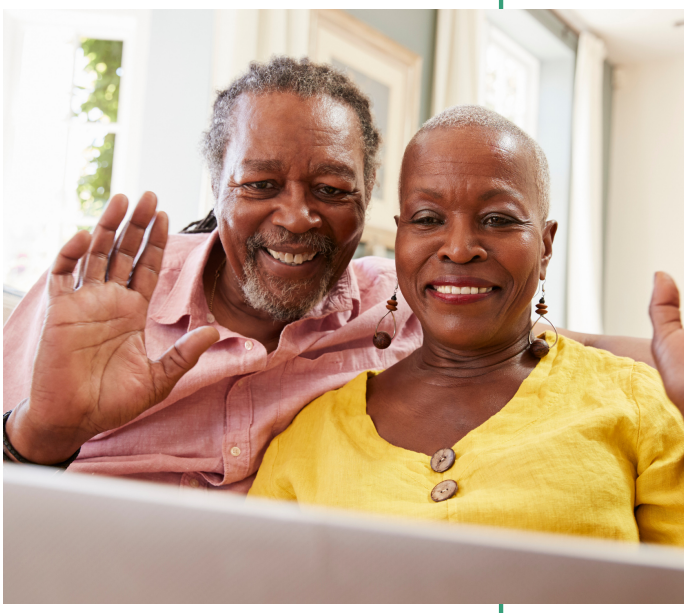
1. Application and systems software such as anti-virus should be updated regularly.

2. The IT department should carry out frequent cyber threat risk assessments.

3. Employees should be trained on how to detect cyber attacks such as phishing and social engineering.

4. Software should be chosen based on strength of privacy policy including third-party agreements, end-to-end encryption and available privacy settings.

PRIVACY IN PRACTICE



Scenario #1

In making the schedule of virtual visits for the week, Sarah creates and prints a document that lists the date, time, resident name, family members' names, email address and phone number.

Considerations: If the file is inappropriately stored or displayed it could be shared accidentally or maliciously.

Scenario #2

Lisa is assisting a resident conduct their virtual family visit. Lisa has known the family for several years and recognizes the participants on the video call. The family members ask about the resident's health since a recent fall.

Considerations: While rapport with residents' families is important, medical information is particularly sensitive and care must be taken to not over share on an insecure platform. There is no way to know if the family is using public wifi or has taken the necessary precautions to secure their network. This type of information would be safer to be shared by medical staff using a more secure method.

Scenario #3

Paul is assisting a resident with their virtual family visit. Paul's facility uses the same laptop for the virtual visits and for the recreational programming.

Considerations: Because the laptop is used for multiple purposes it likely contains several apps and is used by multiple people. Malware that has been accidentally loaded through malicious links in emails or insecure apps could lead to the virtual visit being recorded surrepticiously.

MANAGING PRIVACY BREACHES

- The organization should establish a breach management protocol that details the steps to be taken whenever a breach occurs
- The organization should have a privacy breach policy that provides for the following:
  - The process of identifying privacy/security breaches
  - How to measure the likelihood of a real risk of significant harm to the individuals involved
  - A privacy officer/designated staff primarily responsible for managing such situations
  - Factors to consider in deciding when to report a breach to the Privacy Commissioner
  - A general guide for staff on managing privacy breach situations
  - Steps to mitigate losses/damages resulting from breaches
  - Safeguards to prevent privacy breaches

Resources and Contacts for Assistance:

Family Councils Ontario
www.fco.ngo

Ontario Association of Residents' Councils
www.ontarc.com

Information and Privacy Commissioner of Ontario
www.ipc.on.ca

Office of the Privacy Commissioner of Canada
www.priv.gc.ca

KNOWLEDGEFLOW CYBERSAFETY FOUNDATION

KnowledgeFlow.org

KCF is dedicated to providing no-cost cyber safety information and resources to seniors and youth across Canadian communities regardless of their income, location, ethnicity, gender or sexual orientation.

KnowledgeWise.ca is a repository of tools and resources designed by seniors, for seniors, to empower them to fully engage online safely and securely.

For more resources on using videoconferencing software, visit:

Connect.KnowledgeFlow.org