Administration for Community Living Office of Healthcare Information and Counseling

Managing Through COVID-19 Work grouP - September 2020

Tips for Privacy and Confidentiality: Online vs. Offline

Preparing for Remote Medicare Open Enrollment Toolkit

A picture containing drawing

Description automatically generated A close up of a sign

Description automatically generated A picture containing drawing, food

Description automatically generated

# Overview

This tip sheet provides tips and questions to consider related to privacy and confidentiality when working online vs. offline in programs where grantees and clients would typically meet face-to-face, in the same physical space.

Allowable or unallowable activities are often detailed in written policies and procedures. For example, Volunteer Risk and Program Management *Policy 3.94 - Confidentiality* is a required policy by the U.S. Administration for Community Living (ACL) for State Health Insurance Assistance Programs (SHIPs) and Senior Medicare Patrol Programs (SMPs). Volunteers are responsible for maintaining the confidentiality of all proprietary or privileged information to which they are exposed while serving as a volunteer, whether this information involves a member of staff, a volunteer, a beneficiary or other person, or involves the overall business of the SMP/SHIP.

The key to success for expanding ACL grantee activities to a virtual/remote environment is to emphasize that the same confidentiality rules apply online as when people come together face-to-face in your program. Also note that most of what you need to do online regarding safety and confidentiality involves following procedures, not simply installing an app.

# Considerations

* Look at your current policies and procedures. Do they already cover confidentiality, privacy, and safety? Do they cover permitted and prohibited online activities? Do they cover harassment and complaints process? Do they need to be revised so that they apply both offline **and** online?
* Describe what a violation of confidentiality would look like, both online **and** offline.
* Describe what a violation of safety policies would look like, both online **and** offline.
* Describe in writing exactly what someone should do, in detail, if they observe a violation of safety or confidentiality.
* Consider whether volunteers should use their personal email account for consumer interactions or if they should they create an email account that is used only for their volunteer work. Can your program provide volunteers with agency email addresses? Consider requiring they only use this work email account when working for your program.
* Consider prohibiting volunteers and staff from “friending” a consumer on social media platforms.
* Describe what a volunteer or staff member should do if a consumer starts commenting on their public Tweets, Instagram posts, or other social media. Consider providing an example of how to diplomatically respond if this situation occurs.
* Consider whether volunteers and staff should be required to have a password-protected computer or smart phone if they will use such as a part of their service with your program. Could your program provide guidance on how to do this?
* Consider whether volunteers or staff should be advised to never use a public wi-fi network, even with a Virtual Private Network (VPN), when reading or responding to any messages from their consumer (at an airport, at a coffee shop, at the library, etc.). Should they be told to use a VPN and, if so, who will pay for that and will your IT staff be able to help install it?
* Consider issuing policies or advice regarding what should be showing in the background on a video call with consumers and other team members.
* Consider whether volunteers should use their own Skype, WebEx, GoToMeeting, Zoom account, etc. when working with consumers or if your program will need to develop a platform that can be used by volunteers and staff.

# Tech Tips

* Ask volunteers and staff if the software and operating systems on their computer, smart phone, and/or tablet automatically and regularly updates. If they are not sure, can an IT person from your program talk to them about their devices and determine the answer? It is important to remember that updating software and operating systems helps improve device security.
* Ask volunteers and staff if their devices are password-protected and if anyone else has access to those devices. Could an IT person at your program walk them through how to password-protect their devices if needed?
* Ask volunteers and staff if their home internet access is password-protected, how often they change the password, and how many people have access to their internet. Could an IT person at your program evaluate if they have enough security?