Data security tips for CAREWare MA users to support remote work

April 7, 2020 v1.0

The purpose of this document is to share tips and best practices across organizations to help support data security for program staff that are working remotely during the COVID-19 emergency.[1] This document is organized into six sections: (1) Remote access to CAREWare MA, (2) Limiting external threats; (3) Physical security, including paper files; (4) Protecting electronic data; (5) Transferring or transmitting paper and electronic data; and (6) Destroying data.

1. Remote access to CAREWare MA

- If your organization has a secure Virtual Private Network (VPN), you may be able to access CAREWare MA. Conditions of your CAREWare User Agreement still apply *(a list of these conditions is included at the end of this document)*.
- Staff that cannot use VPN will have to keep track of client session data outside of CAREWare MA.[2]
  - All data recorded in either paper or electronic form (e.g., in a spreadsheet) must be manually entered into CAREWare MA once staff can access the system.
  - Direct service staff that rely on data entry staff should be trained on how to securely store data until they return to the office.

What is Protected Health Information (PHI)? Under the U.S. Health Insurance Portability and Accountability Act (HIPAA), PHI includes any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual. Health care providers need to be especially careful with PHI in any form.

This includes oral communication as well as paper and electronic data. When you talk with clients or discuss client

2. Limiting external threats

- Make sure you have **virus protection software** installed on your computer (whether home or work issued), and that it is up to date. Here is a useful comparison article that includes some free options.
- If you cannot verify that a **wireless network** is secure, it's best to avoid using it. If you must access the internet using a wireless connection, install a firewall directly on the laptop.
- Be cautious about **links and attachments**. Watch out for emails that ask for personal information, and for unusual email addresses and typos. If you get an email from someone you know, with text that doesn't make sense or seems out of character, don't click on anything. Most of all, use extreme caution with attachments. If you aren't sure, contact the sender by phone or separate email.

3. Physical security, including paper files:

- Make sure you are the only person that can see any paper or electronic client information, including while you are working.
  - Do not leave paper files open or unattended. This is especially important in spaces that are shared, or where materials may get picked up by mistake.
- If at all possible, use a **locked storage container, cabinet or suitcase** to store paper files when not in use. Where feasible, physical storage also provides extra security for laptops.
  - Focus on the basics – for example, do not leave keys in a file cabinet lock, and do not share your lock combination with anyone.

[1] Circumstances and resources continue to change across organizations. It is up to your organization to determine which strategies are appropriate and can reasonably be put in place. **Always defer to your organization's policies and procedures around remote work**, as well as to all required state and federal data security regulations.

[2] For security reasons, CAREWare MA requires an agency-specific outgoing IP address that must be pre-approved to allow access.

4. Protecting electronic data

- Separately encrypt and password protect individual electronic files. This is free and easy to do with Microsoft Excel files.
- **Do not save to the cloud!**
  - If you are using a home computer, make sure it is not saving to the cloud. For example, you can turn off syncing completely, or choose which files and folders not to sync for Microsoft OneDrive or iCloud.
  - **Never** use cloud-based files (e.g., Google sheets) or storage (e.g., Dropbox, Google Drive).
- Make sure your computer is set up with a strong password.
  - Do not use this password for anything else. Here's how to reset a Windows password.
  - If you share your computer with other people, set up a separate user account for yourself. Always log out of your account before letting someone else use the same computer.
  - Never share your computer username and password.
  - Consider using a password manager (e.g., LastPass, 1Password) to keep track of passwords. Free options are available. Most can also help you generate strong passwords.
- Save a back-up copy on your computer after each data entry session in case your file gets corrupted or you delete any data by mistake.
- As an extra security measure, you can encrypt your entire computer. Most computers come with the option of whole-disk encryption (e.g., Bitlocker is included with Microsoft Windows, and FileVault2 is included on Macs), but it may need to be enabled.
- Consult with your IT person before installing any software on agency resources.

Which files should be protected? Under HIPAA, PHI includes a list of 18 identifiers, including name, social security number, medical record number, and address. Find all 18 here.

5. Transferring or transmitting paper and electronic data

- Do not send data over regular email.
  What about secure email? If your organization uses secure email (with features such as end-to-end encryption, two-factor authentication, and an SSL certificate) you may be able to use it for data transmission. Check with your IT department to make sure your email service is secure.[3]
- What are some other options for secure data transfer?
  Both paper and electronic data can be hand-carried (on an encrypted device like a laptop or flash drive), sent via dedicated secure fax, emailed using your agency's **secure** email system, or sent by mail.
- Encrypt your data files! This is so important we are saying it again.
- Never transmit data and a password at the same time.

Why shouldn't I send data over regular email? When you send an email, copies are stored in multiple places. This includes any device you have used to send, receive or read email, as well as your internet service provider (ISP), your recipient's computer and their ISP. This applies both to email text and attachments.

6. Destroying data

- Follow your organization's recommendations for data destruction.
- Simply deleting electronic files does not remove or destroy them completely. Data may be saved in other places on the device.
  If you are using a flash drive to transfer electronic data: start by encrypting the entire drive to make its contents unreadable without a key. Then once you've transferred your data, erase it and encrypt it again.
- **Shred** any paper files using a crosscut shredder or secure shredding service.

[3] Many organizations have standards and rules for secure data transmission. Find out if your organization, or other entities that you share data with, prefer or prohibit any specific methods.

Conditions of user account agreement for the Massachusetts CAREWare System

I understand that as a Massachusetts CAREWare system account holder, I agree:

- That the data contained within and used by the CAREWare system include confidential and sensitive information which are protected from unauthorized disclosure under state law, and use of these data are limited by law and by Massachusetts Department of Public Health (MDPH) Confidentiality Policy and Procedures.
- That access to this confidential information is provided for the sole purpose of reporting client-level and service-level data to MDPH and HRSA for clients who receive MDPH-funded services.
- That I will only attempt to look up clients for the purpose of entering the data as it relates to the Ryan White HIV/AIDS Program services and/or state-funded HIV and/or Hepatitis C services the client has received from my agency. (i.e., I will not 'phish' for client names through the CAREWare system).
- That if I view information for which I do not have a Release of Information, I will not divulge any information about those individuals.
- That any information I view is confidential, and I agree not to discuss, transmit, or narrate any such information.
- That I will ensure the physical security of all confidential information when I leave my work area unattended.
- That unauthorized or willful disclosure of confidential information may cause serious harm to individuals and damage to the mission of the Massachusetts Department of Public Health, and will be considered grounds for disciplinary action, up to and including termination and prosecution.
- That my User ID and password is for my exclusive use and may not be loaned to or used by anyone else and I will be accountable for all activities performed under my assigned User ID and password.
- That it is my responsibility to notify JSI by email (CAREWareMAhelpdesk@jsi.com) if I leave the employment of the PROVIDER or no longer require access to CAREWare.
- That I have read, understand, and will comply with all HIPAA regulations and all other applicable state and federal administrative rules, laws and regulations.
- That I will immediately report to JSI by email (CAREWareMAhelpdesk@jsi.com) all incidents of improper access, information misuse, or unauthorized dissemination of information obtained from CAREWare, or anything which leads me to suspect that the security of my own passwords has been compromised.
- That I will comply with the password requirements JSI has in place for access to the CAREWare system.
- That my email address will be added to the CAREWare MA e-newsletter so that I will receive information about important system changes.
- That I will ensure the computer(s) I use to access the CAREWare system are operated in accordance with my employer's IT Security Policies, receive regular operating system patches and virus scans with up-to-date virus definitions, and is otherwise compliant with all of the IT security policies of my employer. *****
- That I will not remove any confidential information obtained as a result of my use of CAREWare from the workplace, nor will I place it on a laptop or portable storage device, or transmit it electronically. *****

***** These last two items may be particularly difficult to follow during remote work. Be sure to follow your employer's IT security policies. Use the tips in this document to help make sure that your devices, electronic data and paper files are protected.