ADMINISTRATIVE PRACTICES MANUAL

Computer and Portable Media Device Policy

PURPOSE

To provide procedures for staff members that use mobile devices to ensure the protection of Protected Health Information (PHI).

PROCEDURE

All computers and portable media devices used to conduct county business will be only those issued by Dane County and staff will not use personally owned computers (with the exception to access a Dane County Citrix Desktop) or portable media devices for county work unless specifically authorized by the Division Manager and/or the HIPAA Privacy and Security Officer. Dane County Information Management provides secured remote access to employees within a Citrix desktop that staff may access on personal owned computers and is considered secured if using only the Citrix desktop and not transferring files between the Citrix desktop and the personally owned computer. The employee must then comply with all requirements given. All data breaches must be reported to the HIPAA Privacy and Security Officer, Dane County Head or designee, and Dane County Information Management (DCIM) and/or Madison's City IT department.

Portable Media Devices include any device or media that is easily portable such as, but not limited to the following:

- Flash Universal Serial Bus (USB) drives, also known as jump drives or thumb drives
- Cell phones, mobile phone, pagers and similar devices when being used for sending and receiving text and/or e-mail messages or storage of verbal communication containing client information (conducting verbal communication via cell phones is permitted)
- Portable hard disk drives
- CDs, DVDs, optical disks, diskettes, magnetic tape and similar media
- Portable dictation devices
- Digital cameras

Employees may use Dane County's webmail portal, but may not download or open attachments from webmail that may contain client/patient confidential or protected health information directly on personal devices or e-mail these types of documents to personal e-mail accounts. Further, employees may not store client/patient protected health information or any other confidential information on any personally owned portable media device, home computer or any other personal device. Employees needing, but not having access to Citrix Dane Desktop should contact his or her supervisor.

Employees may not work on any document containing confidential or protected health information on personally owned cell phones, iPads, tablets, laptops or PCs unless these documents are accessed through the Citrix Dane Desktop, and are not saved locally to the personally owned device.

DCIM direct employees to use the Citrix Sharefile file sharing service to send or store confidential or protected health information. If employees receive information through another file sharing service,

such as DropBox or OneNote, employees are allowed to retrieve the information and must store it in an authorized location.

Employees must password protect all county issued devices that may contain client or patient data. Employees who lose, misplace or know of a county issued computer or portable media device that is stolen or missing, must immediately report this event to his or her supervisor. The supervisor must immediately report the event to the HIPAA Privacy and Security Officer, Dane County Risk Manager, and DCIM staff.

Further, staff that use cell phones for work purposes are required to:

1. Activate and retain a password lock that would be difficult for someone to easily guess.
2. Set up the screen lock feature to go into effect after a short period of inactivity.
3. Turn on the "wipe out" setting that will wipe all information from the phone if the wrong access password is entered more than a set number of times.
4. Do not send PHI via SMS text messages.
5. Refrain from using the device's camera to take and store photos that compromise an individual's confidentiality, unless authorized by Dane County.
6. Ask DCIM for permission to download any applications and receive approval prior to any downloads.
7. To minimize risk of loss, a phone should not be left in a car or unattended.
8. If staff no longer require a device as determined by the program supervisor, or they leave employment, the phone and the accessories must be returned to their supervisor.

DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven years.

ROLES & RESPONSIBILITIES

The HIPAA Privacy & Security Officer is responsible for the implementation, maintenance, and adherence to this policy.

RELATED DOCUMENTS

Definitions
Proper Use of Computer Equipment, Software and Connectivity Policy

DOCUMENT VERSION HISTORY

Original: 08/2023