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

Per the **Proper Use of Computer Equipment, Software, and Connectivity policy** (section 4.7), portable media devices may be used to distribute information to the public or other third parties if it has been classified for public access in terms of the Open Records Act and encryption is not required. Any devices used to conduct County business will be only those issued by Dane County and employees will not use personally owned computers (with the exception of Citrix access, see below under section 4.9) or portable media devices for County work unless specifically authorized by the Division Manager and office of Risk Management. 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). Note - if encryption is required, then it is very likely that the information is not subject to release under Open Records. Purchase of portable media devices for "removable data" must go through DCIM.

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

- Computer laptops, tablets and other portable computers
- 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
- Zip disks, 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.

Employees may not use file sharing or cloud-based services such as DropBox or Google Drive unless the application is County approved by their supervisors in consultation with DCIM helpdesk via email. 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.

Employees that are provided County-issued 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; and
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.

Employees that are provided County-issued computers or laptops for work purposes are required to:

1. Follow the DCIM password policies;
2. Not to share username or passphrase with anyone;
3. Not to use someone else's username or passphrase to gain access;
4. When finished using a computer or device, or when not actively using a computer or device, employees shall log off or lock the computer or device to mitigate the chance of unauthorized access to Dane County systems, PII/PIH, or other data; and
5. Limit access to properly authorized individuals by verifying that any individual doing computer maintenance is authorized to do so.

DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) 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
Updated: 11/2024