ADMINISTRATIVE PRACTICES MANUAL

Facility Access Policy

PURPOSE

To provide procedures to control physical access to and within facilities to safeguard the confidentiality, integrity, and availability of Dane County's Protected Health Information (PHI).

PROCEDURE

Individuals Allowed in Restricted Areas

Restricted areas are areas of Dane County where PHI is stored or utilized. The following people are allowed in restricted areas:

1. Workforce members;
2. Workforce members' family members and friends visiting with the escort of a workforce member as long as PHI is not visible or being discussed;
3. Vendors without a workforce members' escort into and out of the areas for brief periods of time as long as PHI is not visible or being discussed;
4. Vendors on a long-term contract, once acclimated to the areas, without an escort; or
5. Someone going through a restricted area to access an unrestricted area, if escorted by a workforce member.

Facility Security Controls

Authorized workforce members receive access to restricted areas as appropriate for their job duties. Management will provide workforce members and other approved personnel a photo identification (ID) card and an area access card. Use of a county-issued ID or access card for any purpose not directly related to work responsibilities is strictly prohibited. Under no circumstances may an employee lend, share, or give an ID or access card to another person.

A list of individuals with their assigned access is maintained. When an individual's role changes their access will be reviewed to ensure that keys and other lock entry mechanisms continue to be appropriate for the individual's role.

Individuals issued facility keys and other lock entry mechanisms:

1. May not share the keys/access cards or other lock entry mechanisms with any other individual except when authorized.
2. May not permit access to individuals not authorized to enter the building and/or room(s).
3. May only use the keys/access cards or other lock entry mechanisms to enter Dane County's buildings and/or rooms to complete job responsibilities for the organization.
4. Are required to return the keys and other lock entry mechanisms to Dane County on their last day of employment or contracted work.
5. Are required to immediately report when the keys and other lock entry mechanisms are lost, stolen, or otherwise compromised and must initiate an incident report as required in the **Privacy and Security Incident Breach Policy.** Dane County will deactivate the access card, and other lock entry mechanisms, and change locks if necessary.

Exterior access to restricted areas will be secured. Exterior doors with locks on them may not be unlocked and/or be propped open or left unattended at any time except when authorized.

Offsite (Remote) Security Safeguards

Workforce members may not take PHI off premises, unless required by the workforce member's job description or as approved by their supervisor. Workforce members are only authorized to remove the minimum amount necessary to complete their assigned job duties. When PHI is authorized to be taken offsite, workforce members are required to secure the information to prevent unauthorized access, use, and disclosure. PHI must be in the possession of the workforce member and/or in a secure location (e.g., locked container; locked vehicle; locked house) at all times to ensure that only authorized individuals have access to the information.

Additional Safeguards

1. Documents containing PHI should be:
    a. Turned over, covered up, or put away when unattended so it may not be viewed by passersby (including other co-workers);
    b. In locked rooms, cabinets, or drawers when no longer in use;
    c. Removed from printers promptly after being printed; and
    d. Removed from fax machines and distributed to the appropriate recipients promptly.
2. Media containing PHI (e.g., CDs and flash drives) should be in locked rooms, cabinets, or drawers when no longer in use.
3. Computer screens should be locked when unattended (see also **Proper Use of Computer Equipment, Software, and Connectivity** and **Computer and Portable Media Device policies**).
    a. Ensure keys or other lock entry mechanisms are secured so they are not accessible to unauthorized individuals.
4. Workforce Members should report any incident of an unauthorized visitor or unauthorized access to a facility, to their supervisor and the HIPAA Privacy & Security Officer.
5. Do not share or post passwords.

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
Privacy and Security Incident Breach Policy
HR Photo Identification Policy
Proper Use of Computer Equipment, Software, and Connectivity
Computer and Portable Media Device

DOCUMENT VERSION HISTORY

Original: 07/2023

Reviewed: 07/2024