# HIPAA Confidentiality and Privacy Manual

Department of Administration
Updated: January 2026

# Table of Contents

# ADMINISTRATIVE PRACTICES MANUAL

SUBJECT: CONFIDENTIALITY, PRIVACY AND SECURITY

## 1. Introduction

1.1. It is the policy of Dane County to empower every Dane County employee and volunteer working in a covered component to assist in maintaining a professional culture, using practices that respect the confidentiality of protected health information (PHI).

1.2. It is the policy of Dane County to empower every Dane County employee and volunteer working in a covered component, who has any contact (directly or indirectly) with PHI, to use and disclose PHI in accordance with Dane County's HIPAA policies.

1.3. It is the policy of Dane County to empower every Dane County employee and volunteer, regardless of where they work, to assist in maintaining a professional culture, using practices that respect the confidentiality of information covered by other confidentiality laws.

1.4. It is the policy of Dane County to allow each covered component to establish policies and procedures that will supersede this policy if more specific to the functioning of the covered component. For covered components of Dane County government, county-wide policies and procedures control absent more specific department or division HIPAA policies and procedures.

1.5. It is the policy of Dane County that a covered component may not disclose PHI to another part of Dane County government unless the other part of government is a covered component involved in the healthcare, payment or healthcare operations of the covered component; and even then, the exchange of PHI must be limited to the minimum amount necessary for the involved units of government to perform healthcare, payment and healthcare operations.

1.6. Questions regarding the application of Dane County's HIPAA policies or other law protecting confidentiality may be directed to Dane County's HIPAA Privacy and Security Officer and/or the Dane County Office of Corporation Counsel.

HIPAA PRIVACY & SECURITY OFFICER
210 Martin Luther King Jr Blvd., Rm 425
Madison, WI 53703
PH: (608)445-3056

OFFICE OF CORPORATION COUNSEL
210 Martin Luther King Jr Blvd., Rm 419
Madison, WI 53703
PH: (608) 266-4355

## 2. Definitions

2.1 These definitions apply to the Health Insurance Portability and Accountability Act (HIPAA), policies, and forms found throughout this manual. For the full definitions, please refer to the HIPAA Privacy Rules in the Code of Federal Regulations. Always refer to the regulations for the full definitions.

2.1.1 Accounting of Disclosures: Information that describes a covered entity's (CE) disclosures of Protected Health Information (PHI) other than for treatment, payment, and health care operations; disclosures made with authorization; and certain other limited disclosures.

2.1.2 Breach: The impermissible acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the CE or Business Associate (BA), as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

2.1.2.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2.1.2.2 The unauthorized person who used the PHI or to whom the disclosure was made;

2.1.2.3 Whether the PHI was actually acquired or viewed; and

2.1.2.4 The extent to which the risk to the PHI has been mitigated.

Breach excludes:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a CE or BA if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which a CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.1.3 Business Associate (BA): A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity; this includes a sub-contractor that creates, receives, maintains, or transmits PHI on behalf of the BA.

2.1.4 Client/Patient: The individual that is receiving health care or their personal representative.

2.1.5 Covered Entity (CE): An organization that is acting as a health plan, a health care clearinghouse, or a health care provider that transmits any health information in

electronic form for which the U.S. Department of Health and Human Services has adopted a standard.

2.1.6 Covered Component: A part of a Hybrid Entity that would meet the definition of a Covered Entity (CE) or business associate (BA) if that part of the Hybrid Entity was a completely separate legal entity. Dane County is a "Hybrid Entity" as defined under section 45 CFR 164.103 and its Covered Components of Dane County government are listed below.

2.1.7 Data Use Agreement: An agreement that must be entered into before there is a Use or Disclosure of a limited data set to another entity. It establishes the ways in which the information in a limited data set may be used and how it is protected.

2.1.8 Designated Record Set: Any item, collection, or grouping of information that includes PHI and is maintained, collected, Used or disseminated by or for the CE.

2.1.9 Disclose/Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI.

2.1.10 Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

2.1.11 Health Care: Care, services, or supplies related to the health of an individual.

2.1.12 Health Care Operations: Certain administrative, financial, legal, and quality improvement activities of a CE that are necessary to run its business and to support the core functions of treatment and payment.

2.1.13 Health Insurance Portability and Accountability Act (HIPAA): Federal regulations designed to provide privacy standards to protect clients'/patients' medical records and other health information.

2.1.14 Health Oversight Agency: A governmental agency or authority that is authorized by law to oversee the Health Care system, including HIPAA compliance.

2.1.15 HIPAA Privacy & Security Officer: The person designated by Dane County to develop, implement, and oversee the organization's compliance with the Health Insurance Portability and Accountability Act (HIPAA). This person acts as the point of contact for all client/patient privacy issues. They oversee all activities related to the development, implementation, maintenance, and adherence to the covered entity's HIPAA policies and procedures. This person also oversees the management of HIPAA security policies,

procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of the organizational information systems.

2.1.16 Hybrid Entity: A single legal entity:
- 2.1.16.1 That is a covered entity;
- 2.1.16.2 Whose business activities include both covered and non-covered functions; and
- 2.1.16.3 That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D)

2.1.17 Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or there is a reasonable basis to believe the information can be used to identify the individual.

2.1.18 Impermissible Use or Disclosure: Acquisition, use, or disclosure of PHI in a manner not permitted by HIPAA that may or may not compromise the security or privacy of the PHI.

2.1.19 Limited Data Set (LDS): Protected Health Information (PHI) that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
- 2.1.19.1 Names;
- 2.1.19.2 Postal address information, other than town or city, state, and zip code;
- 2.1.19.3 Telephone or fax numbers;
- 2.1.19.4 Electronic mail addresses;
- 2.1.19.5 Social security numbers;
- 2.1.19.6 Medical record numbers;
- 2.1.19.7 Health plan beneficiary numbers;
- 2.1.19.8 Account numbers;
- 2.1.19.9 Certificate/license numbers;
- 2.1.19.10 Vehicle identifiers and serial numbers, including license plate numbers;
- 2.1.19.11 Device identifiers and serial numbers;
- 2.1.19.12 Web Universal Resource Locators (URLs);
- 2.1.19.13 Internet Protocol (IP) address numbers;
- 2.1.19.14 Biometric identifiers, including finger and voice prints; and
- 2.1.19.15 Full face photographic images and any comparable images.

An LDS may include the following PHI:

- Dates such as admission, discharge, service, date of birth, or date of death;
- City, state, 5 digit or more zip code; or
- Ages, in years, months, days or hours

2.1.20 Minimum Necessary: A CE must take reasonable efforts to limit the PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.

2.1.21 Payment: The various activities of a CE to obtain payment or be reimbursed for their services, and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits, and to obtain or provide reimbursement for the provision of health care.

2.1.22 Personal Representative: A person with legal authority to make health care decisions on behalf of a client/patient including: 1) a parent, guardian, or other person acting in loco parentis with legal authority to make Health Care decisions on behalf of the minor child; and 2) a person with legal authority to act on behalf of the decedent or the estate (not restricted to persons with authority to make health care decisions). Within this document the personal representative has all of the rights of the client/patient.

2.1.23 Protected Health Information (PHI): Individually Identifiable health information that is transmitted and/or maintained in electronic or other medium. PHI excludes Individually Identifiable health information in education records covered by the Family Educational Rights and Privacy Act; in employment records held by a covered entity in its role as employer; and regarding a person who has been deceased for more than 50 years.

Typical types of PHI include, but are not limited to, the following:

- Medical records, diagnostic and/or clinical information
- Client/patient demographics or financial information
- Billing and health insurance information

PHI may be in many forms, including, but not limited to the following:

- Verbal communications
- Hard copy records (charts)
- Electronic records
- Notes maintained by staff providing care to the client/patient
- Client/patient sign-in sheets
- Message logs
- Inquiries or information from payers
- Faxed client/patient information
- Diagnostic testing/results
- Data exchanged copies of client/patient information
- E-mails, letters or other client/patient communications

- Specimen containers, prescription labeled bottles, or other Treatment materials that are labeled with PHI.

2.1.24 Sanitization: The removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media.

2.1.25 Secretary: The Secretary of Health and Human Services (HHS) or any other officer or employee to whom the authority involved has been delegated.

2.1.26 Treatment: The provision, coordination, or management of health care and related services among health care providers.

2.1.27 Unsecured Protected Health Information (PHI): PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary.

2.1.28 Use: The sharing, utilization, examination, or analysis of PHI.

2.1.29 Workforce Members: Employees, volunteers, and other persons whose work is under the control of a covered entity or BAA.

Note: Wisconsin State law may have additional or different definitions.

## 3. Overview

3.1 Dane County is a "Hybrid Entity" as defined under section 45 CFR 164.103. "Covered Components" of the hybrid entity are those parts of the government that would meet the definition of a covered entity or business associate if it were a separate legal entity. The Covered Components of Dane County government are as follows:

3.1.1 Dane County Department of Human Services ("DCDHS"). There are eight (8) Divisions within DCDHS. Some Divisions are classified as a "covered component" as defined under section 45 CFR 160.103.

3.1.2 Dane County Department of Emergency Management. Emergency Management involves working with the community to prepare for, respond to, and recover from emergencies. The Division of Emergency Services supports district emergency medical services ("EMS") offices throughout Dane County. Dane County Department of Emergency Management does not itself provide health care or engage in electronic transactions (as contemplated by 45 CFR 160.103), but it is often a Business Associate to each EMS offices which may be are covered entities. Out of an abundance of caution, Emergency Management complies with HIPAA Privacy, Security and Breach Rules.

3.1.3 Dane County Department of Administration ("DOA"). The Department of Administration, including Information Technology and Consolidated Food Services, accesses and handles protected health information created by other county departments, listed above. The Department of Administration particularly processes

invoices for payments of health-related services. The Department, while not defined as a covered component, must follow this policy regarding protected health information it handles from covered components.

3.1.4 Public Health Madison / Dane County ("PHMDC"). As authorized by Wisconsin Statute §251.02(1m), Dane County and the City of Madison jointly created PHMDC as a health department. Certain Divisions of PHMDC are classified as a "covered component" as defined under section 45 CFR 160.103.

3.1.5 The Office of the Dane County Medical Examiner ("ME"). The ME does not provide healthcare, nor does the ME create patient health care records. Therefore, the Office of the ME is not a covered component under section 45 CFR 164.103. It does receive patient health care records that are confidential under Wis. Stat. § 146.82. Therefore, out of an abundance of caution, the Office of the ME complies with HIPAA Privacy, Security and Breach Rules.

3.2 The following Departments are not Covered Components:

3.2.1 The Juvenile Court Program runs the Juvenile Detention Facility and Shelter Home, which contract with an independent healthcare provider to provide health care to residents of the facility. The facility maintains health care information with the healthcare provider. The Juvenile Detention Facility does not conduct electronic transactions as contemplated by section 45 CFR 160.103, and is, therefore, not a covered component. Health records maintained by the facility, however, meet the definition of patient health care records under Wis. Stat. § 146.81(4), and are therefore confidential under Wis. Stat. § 146.82.

3.2.2 Dane County Sheriff's Office ("DCSO"). DCSO contracts with an independent healthcare provider to provide health care to residents of the Dane County jail and to maintain patient health care records that are confidential under Wis. Stat. § 146.82. DCSO does not directly provide healthcare or maintain health care records. While DCSO pays for healthcare, it does not conduct electronic transactions as defined in section 45 CFR 160.103 and is not subject to HIPAA regulations.

3.2.3 Board of Health – Madison/Dane County ("BoH"). The Board of Health is a separate legal entity from Dane County government and is not covered by this policy.

3.2.4 Dane County Regional Airport.

3.2.5 Alliant Energy Center.

3.2.6 Board of Supervisors.

3.2.7 Clerk of Courts.

3.2.8 Corporation Counsel.

3.2.9 Dane County Clerk.

3.2.10 Dane County Executive.

3.2.11 Dane County Treasurer.

3.2.12 Dane County District Attorney's Office.

3.2.13 Family Court Services.

3.2.14 Dane County Highway and Transportation.

3.2.15 Dane County Land and Water Resources.

3.2.16 Dane County Library Services.

3.2.17 Dane County Office of Equity and Inclusion.

3.2.18 Dane County Planning and Development.

3.2.19 Dane County Pretrial Services.

3.2.20 Public Safety Communications.

3.2.21 Dane County Public Works.

3.2.22 Register of Deeds.

3.2.23 Extension Dane County – UW Madison.

3.2.24 Dane County Veteran's Services.

3.2.25 Dane County Waste and Renewables.

3.2.26 Henry Vilas Zoo.

**ADMINISTRATIVE PRACTICES MANUAL**

# Minimum Necessary for Access, Use and Disclosure Policy

## 1. PURPOSE

To limit the use, access, request, and disclosure of Protected Health Information (PHI) to the minimum necessary.

## 2. PROCEDURE

2.1 When using, accessing, requesting, and disclosing PHI, workforce members will limit their use, access, requests for, and disclosure of PHI to the minimum necessary to accomplish their assigned job duties.

2.2 Workforce members will make an individual determination of what amount of PHI meets the minimum necessary standard for requests by considering the requestors purpose and whether de-identified PHI would satisfy the purpose of the request.

2.3 The minimum necessary requirements do not apply in the following circumstances:

- 2.3.1 Requests by or disclosures to a health care provider for treatment;
- 2.3.2 Client/patient requests to access their own information;
- 2.3.3 Information requested and disclosed as a result of an authorization initiated by the client/patient;
- 2.3.4 Disclosures to the Secretary of the U.S. Department of Health and Human Services or related entities such as the Office of Civil Rights;
- 2.3.5 Use and disclosures required by law; and
- 2.3.6 To meet the requirements of HIPAA, such as for the content of standard transactions.

2.4 Workforce members are given access to the PHI needed to perform their job duties through the **Network Access Request Form (NARF)**. Workforce members needing access to PHI should contact their department's DCIM Security Contact to request the change in their access. Workforce members will not use this access to look up their own, their family, or anyone else's PHI unless it is an assigned job duty.

- 2.4.1 When a workforce member's duties change their access will be reviewed and updated.
- 2.4.2 Dane County will make reasonable efforts to use software access controls to limit the workforce members' access to PHI that is necessary to carry out assigned duties.
- 2.4.3 Requests for access to PHI not routinely covered in the scope of the workforce member's position shall be reviewed and approved by their supervisor and/or the department DCIM Security Contact to determine whether the request is appropriate. If the request is for a limited or temporary basis, the workforce member's supervisor shall be responsible for notifying DCIM and/or City of Madison's IT regarding changes in

timeframe or scope of the limited/temporary access using the **Network Access Request Form (NARF)**.

2.4.4 Dane County will monitor access to determine appropriateness of staff access to and use and disclosure of PHI. Methods for auditing access may include:

2.4.4.1 Conducting random spot-checks to determine appropriateness of staff access;

2.4.4.2 Using audits to determine time of access, length of access, access to sensitive or "VIP" client/patient PHI;

2.4.4.3 Reviewing "role-based" access by position and unit of assignment within the organization; or

2.4.4.4 Reviewing requests for and access to "hard copy" client/patient records.

2.4.5 Workforce member access to PHI will be terminated according to **Network Access Request Form (NARF)**.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions

Network Access Request Form

## 6. DOCUMENT VERSION HISTORY

Original: 09/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Identity Verification Policy

## 1. PURPOSE

To ensure that prior to any disclosure of Protected Health Information (PHI) permitted by state or federal law, Dane County verifies the identity of a requesting party and the authority of any such party to have access to PHI.

## 2. PROCEDURE

2.1 If the identity or authority of an individual is not known to Dane County, then Dane County will verify the identity of that individual requesting PHI and the authority of the person to have access to the PHI. Verification of identity and authority will include obtaining documentation, statements, or representations, either oral or written from the requester. Consult the Dane County HIPAA Privacy & Security Officer or request further verification before making any disclosure if uncertain whether or not sufficient verification has been obtained. If needed, verify that appropriate **Authorization for Use and Disclosure of Health Information** is completed.

2.2 The below grid is provided as a guideline for establishing a verification procedure in a variety scenarios.

| **Person to Identify** | **In-Person** | **Telephone** | **Request in Writing** (Fax, mail, hand-delivered) |
|---|---|---|---|
| **Attorney** | Presents with business card or Wisconsin state bar membership and photo identification (i.e., driver's license or organization ID badge). | Ask individual to make written request. | Supplies business card, photo identification (i.e., driver's license or organization ID badge), or letterhead. A confirmatory phone call regarding the requester may be required. |
| **Client/patient** | Client/patient provides at least three pieces of information (e.g., name, date of birth, address, telephone number) or Workforce Member acquainted with parent. | Client/patient provides at least three pieces of information (e.g., name, date of birth, address, telephone number) or Workforce Member acquainted with client/patient | Client/patient provides at least three pieces of information (e.g., name, date of birth, address, telephone number) |
| **Parent of minor child (if there are concerns regarding** | Parent provides client/patient name, | Parent provides client/patient name, | Parent provides client/patient name, |

| Person to Identify | In-Person | Telephone | **Request in Writing** (Fax, mail, hand-delivered) |
|---|---|---|---|
| **custody of the minor child, contact the Dane County HIPAA Privacy & Security Officer)** | address, and date of birth; or<br>Workforce Member acquainted with parent | address, and date of birth; or<br>Workforce Member acquainted with parent | address, and date of birth. |
| **Power of Attorney** | Power of Attorney provides client's/patient's name, address, date of birth, and verifies (via appropriate legal documentation) relationship to client/patient; or<br>Acquainted with Power of Attorney (see F00085) | Power of Attorney provides client's/patient's name, address, date of birth, and verifies (via appropriate legal documentation) relationship to client/patient; or<br>Acquainted with Power of Attorney (see F00085) | Power of Attorney provides client/patient's name, address, date of birth, and verifies (via appropriate legal documentation) relationship to client/patient; or<br>Acquainted with Power of Attorney (see F00085) |
| **Persons involved in the client/patient immediate care** | Client/patient actively involves this person in their care. | Client/patient actively involves this person in their care | N/A |
| **Health care provider from another facility** | Acquainted with Health Care Provider as a Treatment Health Care Provider;<br>Health Care Provider is wearing a photo badge from their facility. | Acquainted with Health Care Provider as a Treatment Health Care Provider; or<br>Call the requestor back through the main number at that facility (instead of through the direct number) | Recognize name of facility and address on letterhead as a Treatment facility; or<br>Call the requestor through the main switchboard number at that facility (instead of through the direct number). |
| **Law enforcement** | Please contact Dane County HIPAA Privacy & Security Officer | Please contact Dane County HIPAA Privacy & Security Officer | Please contact Dane County HIPAA Privacy & Security Officer |
| **Company involved with payment or health care operations** | Recognize requestor/ organization; or<br>Photo identification with organization. | Recognize requestor or call the requestor back through the main number at that facility (instead of through the direct number); or<br>Ask individual to make written request | Recognize name of facility and address on letterhead; or<br>Call the requestor back through the main number at that facility (instead of through the direct number) |

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Authorization for Use and Disclosure of Health Information
Department of Health Services F00085

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Communication Policy

## 1. PURPOSE

To provide procedures for safeguarding Protected Health Information (PHI) transmitted in any form, format or medium, including verbal, written and electronic methods of communication.

## 2. PROCEDURE

### 2.1 Verbal

When communicating PHI verbally, workforce members will do so in private settings with lowered voices. If a client/patient name is needed, only the first name will be used. Workforce members should not use a speakerphone when discussing PHI, and when leaving a message, they should leave a simple message without PHI. Workforce members should only note that their department is calling and leave a call-back number. Workforce members can also leave information necessary to confirm an appointment, but should not disclose what the appointment is for. Further, workforce members should not leave any callback numbers or information in a voicemail that would disclose what the service is for or what services are provided. In these instances, Dane County will need to set up a ghost line to mask the actual number so other people cannot search for the number and determine what a service is for.

### 2.2 Mail

When sending mail to clients/patients, workforce members will ensure the recipient's name and address are correct and put in the correct envelopes. If using envelopes with windows, workforce members will ensure no information other than name and address can be viewed. If other information can be viewed, they should use an envelope without a window.

When sending inter-departmental mail containing PHI, put the document in a regular sealed envelope first addressed to the workforce member. The envelope should be marked "confidential" before putting it into inter-department envelope.

### 2.3 Electronic mail (E-mail)

When sending external emails that include PHI, workforce members will send encrypted emails using the following guidelines:

- 2.3.1 Prior to sending an e-mail to a client/patient, containing PHI, the client/patient must give Dane County consent.
  - 2.3.1.1 Staff should check the client/patient file to verify that there is a completed **Client's/Patient's Right to Request Alternative Communications Form**.
  - 2.3.1.2 If no form has been completed, a workforce member should obtain verbal consent from the client/patient and then complete the **Client's/Patient's Right to Request Alternative Communications Form.**
- 2.3.2 Emails containing PHI must be encrypted. For encryption to occur:
  - 2.3.2.1 PHMDC workforce members must enter "#secure" in the subject line of an email that contains PHI. The subject line can contain other words, but

"#secure" must be somewhere in the subject line. Emails should include discrete, generic subject lines and should not include the client's/patient's name or information about their health or treatment in the subject line. The recipient will receive the email message along with a notice to register a user ID and password, which must be set up in order to access encrypted messages.

2.3.2.1.1 Recipients have three days to access the encrypted message. If they have not accessed the email within three days, the workforce member will need to re-send the message using the encryption process.

2.3.2.2 Dane County workforce members must follow DCIM or City of Madison IT protocol and procedures for sending emails securely (see **Proper Use of Computer Equipment, Software, and Connectivity** policy).

2.3.3 All emails must contain a confidentiality statement, such as: *"This email, including any attachments, may contain confidential or protected health information, which is only for the intended recipient. If you received this email in error, please delete and notify the sender immediately."*

2.3.4 If an external recipient has difficulty opening an encrypted message, that individual should contact the workforce member who sent the message, who will troubleshoot access and contact the Dane County or City IT Helpdesk for assistance if necessary.

## 2.4 Fax

2.4.1 Fax machines should be located in a secure area of Dane County, with no public access. A cover sheet will always be used when faxing client/patient information. Cover sheets should not include any client/patient information. The cover sheet will include the following information:

- Date of the fax;
- Recipient's fax number;
- Name of recipient and their organization
- Name of sender and their contact information (including phone number);
- Number of pages being faxed;
- A confidentiality statement such as: "*CONFIDENTIALITY NOTICE: The information contained in this message is intended only for the private and confidential use of the designated recipient(s) names above, and includes information which should be considered private and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error, and that any review, dissemination, distribution, or copying of this message is strictly prohibited.*

  *If you have received this fax message in error, please notify the sender immediately, and dispose of the confidential information properly, e.g., by shredding or by returning it to the sender. Thank you."*

- Whenever possible, auto-faxing should be utilized for reduction of human errors in dialing the fax numbers. Assigned workforce members should routinely check for faxes and distribute them to appropriate personnel.

## 2.5 Texting

2.5.1 Workforce members in covered components are allowed to communicate with clients/patients through text messaging as long as the messages from workforce members do not contain PHI. If a client/patient name is needed, only the first name will be used.

2.5.2 If a workforce member receives any PHI via a text message, they should transfer a copy of the message or photos into the client/patient file, and delete the message from their device. Workforce members should also notify the client/patient that further transmission of any PHI should be done utilizing one of the other methods of communication.

2.5.3 Please note, some departments/divisions do not allow any type of communication with clients using this method and this policy does not supersede those specific exclusions. Confirm permissibility of these platforms with your supervisor.

## 2.6 Social Media

2.6.1 Workforce members in covered components are highly discouraged from communicating with clients/patients through any social media platform or instant messaging forum (Facebook, Instagram, Snapchat, TikTok, WhatsApp, Twitter, Wink, etc.).

2.6.2 If a client insists on using one of these apps for communication, please follow these guidelines:

2.6.2.1 **Shift to Secure Channels When Possible:** Always aim to move back to more secure and formal communication channels, such as email or our official client portals, as soon as possible. Social media messaging apps should be used as a last resort.

2.6.2.2 **Obtain Written Consent:** As a last resort, employees must secure written consent from the client stating that they are comfortable communicating through their preferred messaging application. This consent form must outline that the client understands the risks involved with using an unprotected platform and acknowledges that any information shared via these apps is not HIPAA-compliant and cannot be guaranteed confidential.

2.6.2.3 **Limit the Use of Messaging Apps:** Even with client consent, please limit the scope of communication on these platforms. Do not send confidential or sensitive information unless absolutely necessary. Use these apps for brief, non-sensitive exchanges only.

2.6.2.4 **Ensure Security Measures:** Be mindful of the security settings on these apps. Enable two-factor authentication and encourage your clients to do the same. Never share passwords, and avoid sending attachments that contain sensitive data unless encrypted.

2.6.2.5 **Document the Communications:** All communications exchanged via social media platforms must be manually documented and added to the client's

official records file. This is necessary as these communications will be considered a record that must be saved in accordance with our retention policies.

2.6.3 Please note, some departments/divisions do not allow any type of communication with clients using this method and this policy does not supersede those specific exclusions. Confirm permissibility of these platforms with your supervisor.

### 2.7 Mitigation and Breach Reporting

When a workforce member becomes aware of misdirected information, they should follow the Privacy and Security Incident and Breach Policy. If a workforce member receives information in error, that person should contact the sender and immediately dispose of the misdirected information.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Computer and Portable Media Device Policy
Privacy and Security Incident and Breach Policy
Dane County Social Media Policy
Proper Use of Computer Equipment, Software, and Connectivity
Client's/Patient's Right to Request Alternative Communications Form
Social Media Use Consent Form

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Reviewed: 07/2024
Revised: 02/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Facility Access Policy

## 1. 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).

## 2. PROCEDURE

### 2.1 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:

- 2.1.1 Workforce members;
- 2.1.2 Workforce members' family members and friends visiting with the escort of a workforce member as long as PHI is not visible or being discussed;
- 2.1.3 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;
- 2.1.4 Vendors on a long-term contract, once acclimated to the areas, without an escort; or
- 2.1.5 Someone going through a restricted area to access an unrestricted area, if escorted by a workforce member.

### 2.2 Facility Security Controls

Authorized workforce members receive access to restricted areas as appropriate for their job duties.

- 2.2.1 Management will provide workforce members and other approved personnel a photo identification (ID) card and an area access card.
- 2.2.2 Use of a county-issued ID or access card for any purpose not directly related to work responsibilities is strictly prohibited.
- 2.2.3 Under no circumstances may an employee lend, share, or give an ID or access card to another person.
- 2.2.4 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.
- 2.2.5 Individuals issued facility keys and other lock entry mechanisms:
  - 2.2.5.1 May not share the keys/access cards or other lock entry mechanisms with any other individual except when authorized.
  - 2.2.5.2 May not permit access to individuals not authorized to enter the building and/or room(s).
  - 2.2.5.3 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.
  - 2.2.5.4 Are required to return the keys and other lock entry mechanisms to Dane County on their last day of employment or contracted work.

2.2.5.5 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.

2.2.6 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.

### 2.3 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.

2.3.1 Workforce members are only authorized to remove the minimum amount necessary to complete their assigned job duties.

2.3.2 When PHI is authorized to be taken offsite, workforce members are required to secure the information to prevent unauthorized access, use, and disclosure.

2.3.3 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.

### 2.4 Additional Safeguards

2.4.1 Documents containing PHI should be:

2.4.1.1 Turned over, covered up, or put away when unattended so it may not be viewed by passersby (including other co-workers);

2.4.1.2 In locked rooms, cabinets, or drawers when no longer in use;

2.4.1.3 Removed from printers promptly after being printed; and

2.4.1.4 Removed from fax machines and distributed to the appropriate recipients promptly.

2.4.2 Media containing PHI (e.g., CDs and flash drives) should be in locked rooms, cabinets, or drawers when no longer in use.

2.4.3 Computer screens should be locked when unattended (see also **Proper Use of Computer Equipment, Software, and Connectivity** and **Computer and Portable Media Device policies**).

2.4.3.1 Ensure keys or other lock entry mechanisms are secured so they are not accessible to unauthorized individuals.

2.4.4 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.

2.4.5 Do not share or post passwords.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. 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 Policy

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Computer and Portable Media Device Policy

## 1. PURPOSE

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

## 2. PROCEDURE

2.1 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.

2.2 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

2.3 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.

2.4 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.

2.5 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.

2.6 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.

2.7 Employees that are provided County-issued cell phones for work purposes are required to:
- 2.7.1 Activate and retain a password lock that would be difficult for someone to easily guess;
- 2.7.2 Set up the screen lock feature to go into effect after a short period of inactivity; and
- 2.7.3 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.
- 2.7.4 Do not send PHI via SMS text messages.
- 2.7.5 Refrain from using the device's camera to take and store photos that compromise an individual's confidentiality, unless authorized by Dane County.
- 2.7.6 Ask DCIM for permission to download any applications and receive approval prior to any downloads.

2.8 Employees that are provided County-issued computers or laptops for work purposes are required to:
- 2.8.1 Follow the DCIM password policies;
- 2.8.2 Not to share username or passphrase with anyone;
- 2.8.3 Not to use someone else's username or passphrase to gain access;
- 2.8.4 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
- 2.8.5 Limit access to properly authorized individuals by verifying that any individual doing computer maintenance is authorized to do so.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 4. RELATED DOCUMENTS

Definitions
Proper Use of Computer Equipment, Software and Connectivity Policy

## 5. DOCUMENT VERSION HISTORY

Original: 08/2023
Updated: 11/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Business Associate (BA) Policy

## 1. PURPOSE

To set forth procedures related to Business Associates (BAs) and Business Associate Agreements (BAAs).

## 2. PROCEDURE

2.1 A Business Associate Agreement (BAA) is needed when Dane County is working with a Business Associate (BA). A BA is a person or entity, other than a workforce member of the county, that creates, receives, maintains, or transmits Protected Health Information (PHI) on behalf of, or provides services to, the covered component for non-treatment management functions, such as claims processing or administration, data analysis, utilization review, quality assurance, billing, legal activities, accounting, consulting, data aggregation management, administrative activities, accreditation activities, or financial services. Program contract managers will determine the entities their department or division contracts with for program related services that require BA contracts. A BA contract addendum will be attached to the standard contract provided for the purchase of services. PHI may be exchanged with BAs who have signed Business Associate Agreements (BAAs) and thus agree to be bound by HIPAA Privacy, Security and Breach Notification Rules.

2.2 When Dane County determines a BAA is needed, workforce members must use the Dane County approved BAA template unless a different BAA is authorized by the Corporation Counsel. BAAs may be stand-alone or made as an addendum to a contract. The BAA must include the following:

- 2.2.1 Establish the permitted and required uses and disclosures of PHI by the BA; and
- 2.2.2 Provide that the BA will:
  - 2.2.2.1 Comply with the requirements of HIPAA that apply to Dane County;
  - 2.2.2.2 Not use or further disclose the information other than as permitted or required by the BAA or as required by law;
  - 2.2.2.3 Use appropriate security safeguards as noted in HIPAA to prevent unauthorized use or disclosure of PHI;
  - 2.2.2.4 Report to Dane County any unauthorized use or disclosure of which it becomes aware, including breaches of unsecured PHI as required by HIPAA;
  - 2.2.2.5 In accordance with HIPAA, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA with respect to such information;
  - 2.2.2.6 Make available PHI in accordance with HIPAA;
  - 2.2.2.7 Make available PHI for amendment and incorporate any amendments to PHI in accordance with HIPAA;
  - 2.2.2.8 Make available the information required to provide an **Accounting of Disclosures** in accordance with HIPAA;

2.2.2.9 Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, Dane County available to the Secretary for purposes of determining Dane County's compliance with HIPAA; and

2.2.2.10 At termination of the BAA, if feasible, return or destroy all PHI created or transmitted under the BA. If such return or destruction is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures.

2.2.3 Authorize termination of the BAA by Dane County, if Dane County determines that the BA has violated a material term of the BAA.

2.3 All PHMDC BAAs will be logged utilizing the City's contract database. All Dane County BAAs will be logged utilizing the County's contract database, MUNIS.

2.4 DCDHS program managers will take steps to ensure that Point of Service ("POS") contractors are in compliance with applicable confidentiality, privacy, security and notice requirements, including but not limited to requirements set forth in HIPAA.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Dane County Department of Human Services standard BAA
City of Madison's standard BAA

## 6. DOCUMENT VERSION HISTORY

Original: 10/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Tracking and Accounting of Disclosures of Protected Health Information (PHI) Policy

## 1. PURPOSE

To set forth procedures for tracking disclosures and responding to requests for an Accounting of Disclosures of PHI.

## 2. PROCEDURE

2.1 Unless exempted by HIPAA, all disclosures must be tracked using the **Disclosure Log.** Disclosures can be in written, verbal and electronic form. Workforce members are not required to track disclosures that are made:

- 2.1.1 For treatment, payment, or health care operations;
- 2.1.2 Directly to the client/patient;
- 2.1.3 Incident to a permitted or required use or disclosure;
- 2.1.4 Under a client's/patient's authorization;
- 2.1.5 To persons involved in the client's/patient's care;
- 2.1.6 For national security or intelligence purposes;
- 2.1.7 To correctional institutions or law enforcement officials with custody over an inmate;
- 2.1.8 As part of a limited data set for research, public health or Health Care Operations; or
- 2.1.9 Seven years prior the date of request.

2.2 When responding to an Accounting of Disclosure:

- 2.2.1 The client/patient may submit a request orally or in writing. All requests must be documented by the client/patient or the Workforce member on the **Request for Accounting of Disclosures Form.**
- 2.2.2 Dane County will act on the request for an accounting and provide the accounting within 60 days after receipt of the request. If Dane County is unable to provide the accounting within 60 days, this time limit may be extended once for up to 30 days if Dane County provides a written statement explaining the reason for the delay and the date by which Dane County will provide the accounting.
- 2.2.3 Each Covered Component will have its own procedure to respond to Requests for an Accounting. The procedure will assign the following to a specific workforce member:
  - 2.2.3.1 A review the **Disclosure Log** to determine whether the client's/patient's record has been disclosed for purposes that must be included in the accounting.
  - 2.2.3.2 A determination as to whether the client's/patient's PHI has been disclosed to a Business Agreement (BA), and if a disclosure to a BA has occurred, then forwarding the **Accounting of Disclosure Requests for Departments and Business Associates Form** to the BA to obtain an accounting of any further disclosures and/or re-disclosures by the BA.

2.2.4 Clients/patients are entitled to one Accounting of Disclosures within a 12-month period at no cost. A fee may be assessed for additional requests. Workforce member(s) will complete the **Disclosure Accounting – Internal** and place it in the client/patient file (or separate file if no client/patient file exists) for tracking purposes and will determine whether Dane County previously provided an Accounting of Disclosures for the client/patient within the past 12-month period. A reasonable, cost-based fee may be charged for subsequent requests during any one 12-month time period. In situations where a fee may be imposed, the requestor will be informed in advance of the fee and given an opportunity to withdraw or modify the request. The workforce member will document the following in the client's/patient's file:

2.2.4.1 the conversation with the requestor about the fee information;

2.2.4.2 the requestor's understanding of the fee information; and

2.2.4.3 the requestor's decision whether to go forward with the Accounting of Disclosures request.

2.2.5 For each disclosure, the following information will be provided:

2.2.5.1 Date of the Disclosure;

2.2.5.2 Name of the entity or person who received the PHI;

2.2.5.3 If known, the address of the entity or person who received the PHI;

2.2.5.4 Brief description of the PHI disclosed; and

2.2.5.5 Brief statement of the purpose of the disclosure or a copy of a written request for disclosure, if any.

2.2.6 For disclosures of PHI to the same person or entity for a single purpose on a repeated basis, the disclosure will include the following information:

2.2.6.1 For the first disclosure: the date, name of entity or person who received the PHI and address, brief description of the PHI and brief statement of the purpose of the disclosure or copy of disclosure request;

2.2.6.2 For subsequent disclosures**:** the frequency or number of disclosures during the accounting period; and the date of the last disclosure during the accounting period.

2.2.7 If the disclosure is for research that involved 50 or more individuals and the requesting client/patient PHI may have been disclosed for a particular protocol or other research activity, Dane County may provide the following information in the accounting instead of the information outlined above:

2.2.7.1 The name of the protocol or other research activity;

2.2.7.2 A description of the research protocol or activity, including the purpose of the research and the criteria for selecting particular records;

2.2.7.3 A brief description of the type of PHI that was disclosed;

2.2.7.4 The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last disclosure;

2.2.7.5 The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the PHI was disclosed; and

2.2.7.6 A statement that the PHI may or may not have been disclosed for a particular protocol or other research activity.

2.2.8 If it is likely that the client's/patient's PHI was used in the research project, Dane County will assist the client/patient in contacting the sponsor of the research and the researcher, if the client/patient requests such assistance.

2.2.9 Complete the **Accounting of Disclosure Response** letter.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Disclosure Log
Request for Accounting of Disclosures
Accounting of Disclosure Response
Accounting of Disclosure Requests for Departments and Business Associates Form
Disclosure Accounting – Internal

## 6. DOCUMENT VERSION HISTORY

Original: 10/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Client Access to Protected Health Information (PHI)

## 1. PURPOSE

To set forth the requirements for processing requests by clients/patients for their own Protected Health Information (PHI).

## 2. PROCEDURE

### 2.1 Processing Requests for Access of PHI

The client/patient is allowed to access to their own PHI. When practicable the client/patient should complete the **Client/Patient Access Request Form.** If the client/patient sends in a written request, that request can be used in lieu of the form. If the client/patient is unable to complete the form, a workforce member should assist in completing the form.

2.1.1 When processing a request for client/patient access to PHI, the following apply:

2.1.1.1 Dane County will act on an access request within 30 days of receipt. If Dane County is unable to complete the request within 30 days of receipt, Dane County is permitted a one-time extension of 30 days for processing the request. If an extension is needed, Dane County will notify the client/patient in writing to explain the reason for the extension and provide a date when the access request will be completed [**Client/Patient Access 30 Day Extension Letter**].

2.1.1.2 Dane County will provide the client/patient with access to the PHI in the form or format requested. If no particular format is requested, when possible, provide document in a PDF format. If the PHI is not readily producible in the requested form or format, Dane County will provide the client/patient with a readable hard copy or electronic form or format as agreed to by Dane County and the client/patient.

- If the client/patient requests the ability to inspect the PHI, Dane County will arrange a mutually convenient time and place for the inspection. Dane County must document the time and date of each request by a client/patient or person authorized by the client/patient to inspect the client's/patient's health care records, the name of the inspecting person, the time and date of inspection, and identify the records released for inspection.
- Upon approval of the client/patient, Dane County may provide a summary of the requested PHI.
- The client/patient may direct Dane County to send the response directly to a third-party designee on their behalf.
- If Dane County does not maintain the PHI requested, but knows where the requested information is maintained, Dane County will inform the client/patient where to direct their access request.

## 2.2 Denial of the Client/Patient Access Request

Dane County may deny access to the client/patient request in limited circumstances. Any denial will be issued within 30 days of the request; be in writing; and include an explanation of the basis for the denial; the client's/patient's appeal rights (if any) and appeal process; and the HIPAA Privacy & Security Officer's contact information.

## 2.3 Reviewable grounds for denial

2.3.1 Dane County may deny a client/patient access to their records, provided that the client/patient is given a right to have such denials reviewed, in the following circumstances:

2.3.1.1 A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the client/patient or another person;

2.3.1.2 The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

2.3.1.3 The request for access is made by the client's/patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such client's/patient's personal representative is reasonably likely to cause substantial harm to the individual or another person

2.3.2 The client/patient has the right to have the denial reviewed by a licensed health care professional who is designated by Dane County to act as a reviewing official and who did not participate in the original decision to deny. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested. Dane County must promptly provide written notice to the client/patient of the determination of the designated reviewing official and take other action as required to carry out the designated reviewing official's determination.

## 2.4 Unreviewable grounds for denial

Dane County may deny client/patient access to their records without providing the client/patient an opportunity for review in the following circumstances:

2.4.1 The request is for psychotherapy notes;

2.4.2 The request is for information compiled in reasonable anticipation of, or for use in, a legal proceeding;

2.4.3 Dane County, when acting under the direction of a correctional institution, may deny, in whole or in part, a client/patient, who is under custody of the correctional institution, request to obtain a copy of their PHI if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the client/patient or of other individuals under the custody of a correctional institution, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transport of the client/patient;

2.4.4 A client's/patient's access to PHI created or obtained by Dane County in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the client/patient has agreed to the denial of access when consenting to participate in the research that includes treatment, and Dane County has informed the client/patient that the right of access will be reinstated upon completion of the research;

2.4.5 A client/patient's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law; or

2.4.6 Client's/patient's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Client/Patient Access Request Form
Client/Patient Access 30 Day Extension Letter

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Revised: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Disclosure of Protected Health Information (PHI) to Non-Clients

## 1. PURPOSE

To set forth the requirements for when Protected Health Information (PHI) may be disclosed to an authorization, and when an authorization is needed.

## 2. PROCEDURE

2.1 Each Dane County covered component may use and disclose PHI for treatment, payment, and health care operation activities without an individual's authorization.

2.2 Each Dane County covered component is permitted, but not required, to use and disclose PHI without an individual's authorization or permission in the following circumstances:

- 2.2.1 As Required by Law (including by statute, regulation, or court orders).
- 2.2.2 For Public Health Activities:
  - 2.2.2.1 public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
  - 2.2.2.2 entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance;
  - 2.2.2.3 individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and
  - 2.2.2.4 employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.
- 2.2.3 For reporting concerns regarding victims of abuse, neglect or domestic violence. Dane County may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.*
- 2.2.4 Health Oversight Activities. PHI may be disclosed to health oversight agencies for purposes of legally authorized activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.
- 2.2.5 Judicial and Administrative Proceedings. Dane County may Disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.
- 2.2.6 Law Enforcement Purposes. Dane County may disclose PHI to law enforcement officials under the following circumstances:

2.2.6.1 as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
2.2.6.2 to identify or locate a suspect, fugitive, material witness, or missing person;
2.2.6.3 in response to a law enforcement official's request for information about a victim or suspected victim of a crime;
2.2.6.4 to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
2.2.6.5 when there is a belief that PHI is evidence of a crime that occurred on its premises; and
2.2.6.6 in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

2.2.7 Decedents. PHI may be disclosed to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

2.2.8 Cadaveric Organ, Eye, or Tissue Donation. PHI may be disclosed to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

2.2.9 Research. PHI may be disclosed for research that is allowed by HIPAA and authorized by the HIPAA Privacy & Security Officer.

2.2.10 Serious threat to health or safety. PHI may be disclosed if necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). PHI may also be disclosed to law enforcement officials if the information is needed to identify or apprehend an escapee or violent criminal.

2.2.11 Essential government functions. PHI may be disclosed for certain essential government functions including:
2.2.11.1 assuring proper execution of a military mission;
2.2.11.2 conducting intelligence and national security activities that are authorized by law;
2.2.11.3 providing protective services to the President;
2.2.11.4 making medical suitability determinations for U.S. State Department employees;
2.2.11.5 protecting the health and safety of inmates or employees in a correctional institution; and
2.2.11.6 determining eligibility for or conducting enrollment in certain government benefit programs.

2.2.12 Workers' compensation. PHI may be disclosed as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

2.2.13 Whistleblower Protections. It is not a violation of HIPAA regulations for a workforce member or business associate to disclose limited protected health information in the course of a complaint against the department, provided the following steps are taken:
2.2.13.1 The workforce member or business associate believes in good faith that the department has engaged in conduct that is unlawful or otherwise violated

professional standards, or that the care, services, or conditions provided by the department potentially endangers clients, workers, or the public; and

2.2.13.2 The disclosure is to a health oversight agency or public health authority authorized by law to investigate or oversee the relevant conduct or conditions complained of or an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct complained of.

2.3 If the client/patient is requesting to release information to someone other than themselves, the client/patient must complete the **Authorization for Use and Disclosure of Health Information** form. If the client/patient is requesting their own records, please see the **Client/Patient Access Request to Protected Health Information (PHI) Policy.**

2.3.1 An authorization to release PHI must be written in plain language.

2.3.2 A valid authorization must contain the following core elements/information:

2.3.2.1 Client's/patient's full name and date of birth;

2.3.2.2 Meaningful description of the information Used or Disclosed (i.e., specific date of service, clinic visit, etc.);

2.3.2.3 Identification of person/agency to whom the covered component is authorized to make the requested use or disclosure (i.e., name, address);

2.3.2.4 Description of the purpose for the use or disclosure ("at the request of the individual" is sufficient);

2.3.2.5 The authorization's expiration date or expiration event;

2.3.2.6 A statement of the client/patient's right to revoke the authorization (except where Dane County has already acted in reliance on the authorization) in writing and how this can be done;

2.3.2.7 A statement that information used/disclosed under the authorization may be subject to re-Disclosure by the recipient;

2.3.2.8 The signature of the client/patient and date of signature; and

2.3.2.9 A statement that treatment, payment, enrollment, and eligibility for benefits cannot be conditioned on whether the individual signs the authorization.

2.3.3 Invalid/Defective Authorizations

2.3.3.1 An authorization to use/disclose PHI is not valid if any of the following circumstances are present:

- The expiration date has passed or the expiration event is known by the covered component to have occurred;
- The authorization has not been filled out completely with respect to the required core elements;
- The authorization is known to have been revoked in writing;
- The authorization is a prohibited type of combined authorization;
- The authorization conditions treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization; or
- Any material information in the authorization is known by the covered component to be false.

2.3.3.2 Defective authorizations will be returned to the individual with an explanation of why the authorization will not be honored.

2.3.4 A copy of the signed **Authorization for Use and Disclosure of Health Information** must be offered to the individual.

2.3.5 Revocation of Authorization. A client/patient may revoke **Authorization for Use and Disclosure of Health Information** form by submitting a written request to Dane County utilizing the **Revocation of Authorization for Use and Disclosure of Health Information** form. Except to the extent that the covered component has already used or released information while the authorization was still valid. Upon receipt of the request to revoke authorization, the covered component will no longer use or disclose (with the exception of information for treatment, payment or health care operations or other instances where an authorization is not required).

## 3. DOCUMENTATION

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

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Authorization for Use and Disclosure of Health Information
Revocation of Authorization for Use and Disclosure of Health Information
Client/Patient Access Request to Protected Health Information (PHI) Policy

## 6. DOCUMENT VERSION HISTORY

Original: 10/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Amendment of Protected Health Information (PHI) BY Clients

## 1. PURPOSE

To set forth the requirements for processing client/patient requests to amend Protected Health Information (PHI).

## 2. PROCEDURE

### 2.1 Request for Amendment of PHI

2.1.1 A request for amendment will be documented in writing by the client/patient or workforce member on the **Amendment Request Form**. The request will identify the information to be amended and supporting reasons for the amendment.

2.1.2 Dane County will act on the client's/patient's request for amendment no later than 60 days after receipt of the amendment. Dane County is permitted to have a one-time extension of 30 days for processing the amendment if the client/patient is given a written statement [**Amendment Request 30 Day Extension Letter**] of the reason for the delay and the date by which the amendment request will be processed.

### 2.2 Acceptance of Amendment Request

2.2.1 If Dane County accepts the client's/patient's request, Dane County will:

2.2.1.1 Make the appropriate amendment to the PHI as indicated in the request;

2.2.1.2 Inform the client/patient using the **Amendment Request Response** that the amendment request is accepted; and

2.2.1.3 Within a reasonable timeframe, make reasonable efforts to provide the amendment to:

- Persons/entities that Dane County knows have the PHI that is the subject of the amendment and may have relied on or could foreseeably rely on the information; or
- Anyone identified by the client/patient as having received PHI.

### 2.3 Denial of Amendment Request

2.3.1 A request for an amendment may be denied if the PHI requested to be amended:

2.3.1.1 Was not created by Dane County and the originator of the information is available to make the amendment;

2.3.1.2 Is not part of the Designated Record Set;

2.3.1.3 Is not supported by a reason;

2.3.1.4 Is not accessible to the client/patient because federal and/or state law prohibit access; or

2.3.1.5 Was accurate and complete at the time of documentation.

2.3.2 If a client/patient's request for amendment is denied, Dane County will provide the client/patient with a written denial using the **Amendment Request Response** that contains:

2.3.2.1 The basis for the denial;

2.3.2.2 Notification of the right to submit a written statement disagreeing with the denial and how the client/patient may file such a statement;

2.3.2.3 A statement that if the client/patient does not submit a statement of disagreement that the individual may request that Dane County provide the **Amendment Request Form** and the denial with any future disclosures of the client's/patient's PHI that was the subject of the request;

2.3.2.4 A description of how the client/patient may file a complaint with Dane County or the Secretary; and

2.3.2.5 The name or title, and telephone number of the HIPAA Privacy & Security Officer.

### 2.4 Written Statement of Disagreement

If the client/patient does not agree with the denial, they may submit a written statement disagreeing with the denial and the basis for such disagreement. If a statement of disagreement is received, Dane County also append or otherwise link the statement to the records subject to the disagreement, and Dane County will include the material appended, with any subsequent disclosure of the PHI to which the disagreement relates.

### 2.5 Rebuttal of Statement of Disagreement

Dane County will prepare an **Amendment Request Rebuttal** to the written statement of disagreement, which will be provided to the client/patient. Dane County will append or otherwise link the rebuttal to the records that is the subject of the disagreement.

### 2.6 Partial Acceptance/Partial Denial of Amendment Request

When a request for amendment is accepted in part and denied in part, the two parts will be treated separately. The accepted component will be treated in accordance with the section of this policy titled "Acceptance of Amendment Request". The denied component will be treated in accordance with the section of this policy entitled: "Denial of Amendment Request."

### 2.7 Amendments from Other Covered Entities (CE)

If Dane County receives notification from another CE that an individual's PHI has been amended, Dane County will ensure that amendments are made to the client's/patient's record; and will inform its Business Associates (BAs) that may use or rely on the client's/patient's record of the amendment so that the BAs can make the necessary revisions based on the amendment.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Amendment Request Form
Amendment Request Response
Amendment Request 30 Day Extension Letter
Amendment Request Rebuttal

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Client Request to Restrict the Use and/or Disclosure of Protected Health Information (PHI)

## 1. PURPOSE

To set forth procedures for requests to restrict the use and disclosure of Protected Health Information (PHI).

## 2. PROCEDURE

### 2.1 Request for Restriction of Use or Disclosure of PHI

2.1.1 A request for a restriction will be completed by the client/patient or the workforce member using the **Restriction Request Form** and should be given to the HIPAA Privacy & Security Officer.

2.1.2 The Dane County covered component will respond to the request within 60 days whether the request will be granted.

2.1.3 The Dane County covered component may approve a client's/patient's request to restrict disclosure of PHI:

- 2.1.3.1 For the purpose of treatment, payment or health care operations;
- 2.1.3.2 To person's involved in the client's/patient's health care; or
- 2.1.3.3 To notify family members or others about the client's/patient's general condition, location or death.

2.1.4 The Dane County covered component is not required to agree to the restriction unless the disclosure:

- 2.1.4.1 it is to a health plan for purposes of carrying out payment or health care operations (not for treatment);
- 2.1.4.2 not otherwise required by law; and
- 2.1.4.3 PHI that pertains to a health care item or service for which the health care provider involved has been paid out-of-pocket in full by an individual.

2.1.5 If the agreed upon restriction(s) hampers treatment, a workforce member may ask the individual to modify or revoke the restriction(s). The Dane County covered component may require written agreement to the modification/revocation or document the client/patient's oral agreement. If the client/patient does not agree to the modification or revocation, the Dane County covered component can deny the request (as long as section 4 above does not apply).

2.1.6 If the Dane County covered component grants the restriction, then the covered component will:

- 2.1.6.1 Notify the client/patient that the request has been granted utilizing the **Response to Request for Restriction** form.
- 2.1.6.2 Ensure the restriction is documented in the client's/patient's record in a manner that ensures compliance with the restriction. The Dane County covered component will flag documents with any PHI pertaining to out-of-pocket

restrictions to ensure restricted PHI is not inadvertently disclosed for payment or health care operations purposes.

2.1.6.3 The Dane County covered component will inform the individual that the restriction(s) will be honored with the following exceptions:

- Emergency treatment situations in which Dane County may use or disclose information to a health care provider for providing treatment. Dane County will request that the emergency treatment provider not further use or disclose the information;
- The restriction is terminated by either the Dane County covered component or the client/patient;
- To the extent applicable, if restrictions prevent uses or disclosures permitted or required under HIPAA.
- Where the PHI requested for restriction was used, disclosed, or released prior to the request.

2.1.7 If a client's/patient's restriction request includes PHI received from an external entity, the client/patient will be directed by the Dane County covered component to the entity or organization where the PHI originated.

2.1.8 The Dane County covered component will notify any Business Associate to which the restriction(s) may apply.

2.1.9 If the request for restriction is denied, The Dane County covered component will complete the **Response to Request for Restriction** form.

### 2.2 Emergency Situations

2.2.1 Emergency situations are circumstances in which The Dane County covered component may use or disclose PHI in a manner contrary to an agreed upon restriction. In order to use or disclose the PHI in an emergency situation, the following must occur:

2.2.1.1 The client/patient that requested the restriction must be in need of emergency treatment, and the restricted PHI must be necessary to provide the emergency treatment.

2.2.1.2 The Dane County covered component will inform the emergency treatment health care provider that they may not further use or disclose the restricted PHI.

### 2.3 Termination of Restriction

2.3.1 Dane County may terminate restrictions when the client/patient requests the termination in writing, or the client/patient orally requests the termination and a workforce member documents the termination. If Dane County is going to terminate the restriction, Dane County must inform the client/patient. Dane County's termination is only effective for PHI created or received after the termination notice is provided and only when Dane County is not required to agree to the restriction.

## 3. DOCUMENTATION

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

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Restriction Request form
Response to Request for Restriction form

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# De-Identification Policy

## 1. PURPOSE

To establish procedures for de-identifying (also known as redacting) Protected Health Information (PHI) to allow for its use and disclosure.

## 2. PROCEDURE

2.1 If PHI is de-identified, it is no longer considered PHI and can be used or disclosed without a client's/patient's authorization. For PHI to be considered de-identified, it must undergo the following process:

2.1.1 Identifier Removal – All of the following elements are removed from the records:

2.1.1.1 Names;

2.1.1.2 All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

- The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

2.1.1.3 All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

2.1.1.4 Telephone or fax numbers;

2.1.1.5 Electronic mail addresses;

2.1.1.6 Social Security numbers;

2.1.1.7 Medical record number;

2.1.1.8 Health plan beneficiary numbers;

2.1.1.9 Account numbers;

2.1.1.10 Certificate/license numbers;

2.1.1.11 Vehicle identifiers and serial numbers, including license plate numbers;

2.1.1.12 Device identifiers and serial numbers;

2.1.1.13 Web Universal Resource Locators (URLs);

2.1.1.14 Internet Protocol (IP) address numbers;

2.1.1.15 Biometrics identifiers, including finger and voice prints;

2.1.1.16 Full face photographic images and any comparable images; and

2.1.1.17 Any other unique identifying number, characteristic, or code.

2.1.2 If, after de-identifying the PHI under step one, the information used alone or in combination with other information, could be used to identify the client/patient, then the de-identified information may still not be disclosed.

2.1.3 A unique identifier is an identifier that only means something to Dane County, such as a sequentially generated record number, may be included with the de-identified information. Unique identifiers allow:

2.1.3.1 The recipient of a group of records to list clients/patients without learning their identity;

2.1.3.2 Dane County to later re-identify (or link) the health information back to the client/patient; and

2.1.3.3 Re-identifiers are only used if the unique identifier:

- Is not disclosed to the recipient;
- Is not derived from or related to any part of the identifiers listed in item 1 above; and
- Has meaning only to Dane County.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Limited Data Set (LDS) Policy

## 1. PURPOSE

To establish procedures for utilizing a Limited Data Set (LDS).

## 2. PROCEDURE

2.1 An LDS may be used or disclosed only for the purposes of research, public health oversight, or health care operations and only when there is a Date Use Agreement in place. All users of an LDS will comply with the minimum use requirements. A LDS does not need to be recorded in the **Accounting of Disclosure Log.**

2.2 Prior to disclosing a LDS, a Data Use Agreement must be in place and contain the following information:

- 2.2.1 Establish the permitted uses and disclosures of the LDS;
- 2.2.2 Identify who may use or receive the information
- 2.2.3 Prohibit the recipient from using or further disclosing the information, except as permitted by the Data Use Agreement or as permitted by law;
- 2.2.4 Require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the Data Use Agreement;
- 2.2.5 Require the recipient to report to Dane County any unauthorized use or disclosure of which it becomes aware;
- 2.2.6 Require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the Data Use Agreement; and
- 2.2.7 Prohibit the recipient from identifying the information or contacting the clients/patients.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Destruction and Disposal of Protected Health Information (PHI)

## 1. PURPOSE

To ensure the proper destruction and disposal of Protected Health Information (PHI).

## 2. PROCEDURE

2.1 Material containing PHI will be destroyed or disposed of pursuant to **Dane County's General Records Schedule**.

2.2 Material containing PHI that will be destroyed or disposed of should be secured against unauthorized or inappropriate access until the destruction or disposal of the PHI.

2.3 Allowable disposal methods for PHI in paper records includes shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. If a locked bin is available, place all paper records to be shredded in a locked shredder bin for proper disposal.

2.4 Remove and shred labels from prescription bottles.

2.5 For destruction of PHI on electronic media options include: clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Dane County General Records Schedule

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Reviewed: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Security Policy

## 1. PURPOSE

To ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) and protected health information (PHI) it creates, receives, maintains, or transmits.

1.1 In furtherance of this goal, Dane County has designated the HIPAA Privacy & Security Officer within the Department of Administration, Division of Risk Management as our HIPAA Security Officer.

1.2 Except for PHMDC, Dane County's HIPAA Privacy & Security Officer works with Dane County's Chief Information Officer (CIO) to coordinate all HIPAA security development, implementation and oversight.

1.3 Pursuant to an intergovernmental agreement between Dane County and the City of Madison, Dane County's HIPAA Privacy & Security Officer works with a City of Madison IT liaison to coordinate all HIPAA security development, implementation and oversight with regard to Public Health – Madison/Dane County (PHMDC).

## 2. PROCEDURE

Dane County's CIO and City of Madison IT liaison will implement standard operating procedures to ensure compliance with HIPAA Security requirements.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Intergovernmental Agreement creating PHMDC

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Revised: 07/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Privacy and Security Incident and Breach Policy

## 1. PURPOSE

To establish processes and procedures to handle privacy and security incidents and breaches of Protected Health Information (PHI).

## 2. PROCEDURE

2.1 Any Dane County employee who becomes aware of a potential improper use, access, and disclosure of PHI is required to immediately:

- 2.1.1 Limit any further improper use, access, and disclosure; and
- 2.1.2 Report the matter to their supervisor, who should report the incident to the HIPAA Privacy & Security Officer, Dane County Risk Manager, and the designee from the Dane County Corporation Counsel Office.
  - 2.1.2.1 All reports should be sent to HIPAA@danecounty.gov.
  - 2.1.2.2 For staff at DCDHS this is done by including the #HS BIGCAT distribution list in the email "To" section.

2.2 Incident investigation. Upon receipt of incident report, the HIPAA Privacy & Security Officer will investigate the incident to determine whether an incident or a breach occurred. This investigation may include obtaining additional information from supervisors or employees. Findings will be documented in the **Privacy and Security Assessment Report.**

- 2.2.1 If the report is determined to not be an incident, the HIPAA Privacy & Security Officer will notify all involved parties and close the report with no further actions.
- 2.2.2 If it is determined to be a breach, the HIPAA Privacy & Security Officer will notify all parties involved, complete all required breach notifications, and close the report. The HIPAA Privacy & Security Officer will also follow up with the supervisor/manager to gather information on what follow up actions were taken with the employee involved in the breach and document this for reporting to the U.S. Department of Health and Human Services (HHS) as required by law.

### 2.3 Breach Notifications

- 2.3.1 The HIPAA Privacy & Security Officer will immediately notify the Risk Manager of the breach to determine if notification of cyber insurance carrier is necessary.
- 2.3.2 A breach is treated as discovered on the first day when an incident that could be a breach is known, or if by exercising reasonable diligence would have been known, to Dane County or any Business Associate (BA).
- 2.3.3 Notifications will be completed or reviewed by the HIPAA Privacy & Security Officer.
  - 2.3.3.1 Notice must be provided to the affected client(s)/patient(s) without unreasonable delay, and in no case, no later than 60 days after the discovery of the breach by Dane County or the BA. Notice will be provided in the following form:

- Written notification by first-class mail to the client/patient at the last known address of the individual or by email if the client/patient has agreed to electronic communications. If Dane County knows that the client/patient is deceased, it will notify the next of kin or personal representative.
- Substitute Notice:
    - In a case where there is insufficient or out-of-date contact information for fewer than 10 clients/patients, the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
    - In the case in which there is insufficient or out-of-date contact information for 10 or more clients/patients, the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of Dane County's website, or a conspicuous notice in media outlets in Dane County's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where individuals can learn whether their PHI may be included in the breach.
- If the Department determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

2.3.4 Where less than 500 individuals are affected, notifications must be made to Secretary (HHS) no later than 60 days after the end of that calendar year in which the breach(es) were discovered.

2.3.5 Where 500 or more individuals are affected, notifications must be made to the Secretary (HHS) and the media without unreasonable delay, and in no case, no later than 60 calendar days after the discovery of the breach. For the media, notice must be provided in the form of a press release to prominent media outlets serving the geographic areas where the individuals affected by the breach likely reside.

2.3.6 The notice shall be written in plain language and must contain the following information:

2.3.6.1 A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2.3.6.2 A brief description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, diagnosis, disability code or other types of information were involved).

2.3.6.3 Any steps the client/patient should take to protect themselves from potential harm resulting from the breach.

2.3.6.4 A brief description of what Dane County did to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

2.3.6.5 Contact information for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or a postal address.

2.3.6.6 If a law enforcement official states to Dane County that a notification would impede a criminal investigation or cause damage to national security, the Department will:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification for the time period specified by the law enforcement official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification temporarily but no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

## 2.4 Mitigation

2.4.1 The HIPAA Privacy & Security Officer will work with appropriate staff to determine if any updates are needed to policies or procedures to reduce the risk of a similar incident or breach occurring in the future. Mitigation efforts will take place as soon as possible after the incident or breach. If the incident or breach involves a security incident, the HIPAA Privacy & Security Officer will work Dane County Information Management or City of Madison IT (as appropriate) to mitigate the risk of future incidents or breaches.

## 2.5 Discipline

2.5.1 Under HIPAA, covered entities are obligated to "impose and document appropriate sanctions" against employees who are found to have violated HIPAA privacy policies. This means Dane County must address the violation with employees who breach PHI. The severity of response is based on the severity of the breach. The department for whom the employee works is responsible for determining the action to be taken consistent with this policy. With that in mind, the below has been developed to guide the HIPAA Privacy & Security Officer in determining the level of severity:

2.5.1.1 **Level 1-Careless, Unintentional, Inadvertent**

The first level is a careless, unintentional, or inadvertent access, review, or disclosure which could include things like misdialing a fax number, entering an incorrect email address, or putting PHI letters in wrong envelopes.

2.5.1.2 **Level 2-Intentional-No Malice or Personal Gain**

The second level is when an employee intentionally accesses, reviews, or discloses PHI without authorization and does so without any personal malice or for personal gain. Examples could include looking at a celebrity's medical record or accessing and reviewing a patient's medical record out of concern or curiosity.

2.5.1.3 **Level 3-Intentional-Malice or Personal Gain**

The third level is when an employee intentionally accesses, reviews, discloses, or uses PHI for personal gain or with a malicious intent.

2.5.2 Recommendations for action, based on the appropriate level of severity, include:

2.5.2.1 **Level 1:** Additional training and/or a documented Coaching Note. Employees having multiple infractions may warrant a disciplinary action.

2.5.2.2 **Levels 2 and 3**: A Pre-Disciplinary Letter must be issued, which constitutes notice of a scheduled meeting. Outcomes could include discipline, ranging from a letter of reprimand up to and including termination of employment. Employee Relations should be consulted to assist in the determination of the level of discipline to be imposed.

2.5.3 It is important to note, these are recommendations and not requirements. The specific action imposed in any particular case will, however, depend on the facts.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions

*Employee Benefit Handbook

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023

Updated: 01/2025

Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Workforce Members Training Policy

## 1. PURPOSE

To ensure workforce members are trained on all required HIPAA requirements, policies and procedures.

## 2. PROCEDURE

2.1 New hire training: Workforce members will be trained on HIPAA's privacy and security requirements and HIPAA policies and procedures through NeoGov Learn LMS as a part of the onboarding process.

2.2 Annual Training: Workforce members identified as staff who handle confidential or PHI will receive annual training on the topics of privacy, security and confidentiality through NeoGov Learn LMS.

2.3 Updates, reminders, and additional training: Workforce members will receive updates, reminders, and/or training when there are material and relevant changes to HIPAA or any privacy and security policies or procedures or if reminders are needed about current policies.

2.4 Workforce members will be evaluated on their understanding of the HIPAA Protections and Compliance training.

2.5 Completion of the HIPAA Protections and Compliance training will be tracked and monitored through NeoGov Learn LMS.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions

## 6. DOCUMENT VERSION HISTORY

Original: 07/2023
Reviewed: 07/2024
Revised: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# Privacy Practices Audit Policy

## 1. PURPOSE

To establish controls and periodic reviews to monitor access, use, and disclosure of Protected Health Information (PHI).

## 2. PROCEDURE

2.1 Dane County performs internal audits to measure compliance with HIPAA regulations, policies and procedures. The audits will be conducted by the HIPAA Privacy & Security Officer. The types of audits should check for compliance with policies, practices and procedures such as:

- 2.1.1 Documentation of **Notice of Privacy Practices (NPP)** provided to client/patient at first point of contact;
- 2.1.2 Appropriate posting of **NPP;**
- 2.1.3 Incident/Breach procedures being followed;
- 2.1.4 Workforce member privacy training;
- 2.1.5 PHI access, use, and disclosure;
- 2.1.6 Secure e-mail messaging used when sending PHI;
- 2.1.7 Business Associate (BA) compliance with the Business Associate Agreement;
- 2.1.8 Information system activity, such as logs and access reports; or
- 2.1.9 Compliance with specific rules and areas that have been the focus of particular attention on the part of the federal Office for Civil Rights (OCR).

2.2 Following any audit that reveals compliance issues, Dane County will take corrective action to ensure future compliance with HIPAA regulations, policies, and procedures. Audits and any corrective action must be documented.

### 2.3 Audit Techniques

Audit techniques may include:

- 2.3.1 Workforce member interviews;
- 2.3.2 File reviews;
- 2.3.3 Questionnaires submitted to BAs;
- 2.3.4 Facility walk-throughs; and
- 2.3.5 Monitoring access and use of electronic records, and electronic systems.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Notice of Privacy Practices

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Reviewed: 09/2024
Reviewed: 01/2026

**ADMINISTRATIVE PRACTICES MANUAL**

# HIPAA Complaint Policy

## 1. PURPOSE

To set forth procedures to investigate external complaints related to a client's/patient's privacy rights and whether Dane County's HIPAA policies and procedures have been violated.

## 2. PROCEDURE

### 2.1 Reporting

An individual may call, e-mail, write, or appear in person to Dane County with a complaint. If the individual does not complete the **Complaint Form,** a workforce member will assist in the completion of the form.

- 2.1.1 The **Complaint Form** will include:
  - 2.1.1.1 The individual's name and contact information;
  - 2.1.1.2 Description of the complaint;
  - 2.1.1.3 Documentation that supports the reported incident (if available); and
  - 2.1.1.4 Information on how to make a complaint to the Secretary.
- 2.1.2 The completed **Complaint Form** will be sent to the HIPAA Privacy & Security Officer.

### 2.2 Investigation & Response

The HIPAA Privacy & Security Officer will review the **Complaint Form** and will follow the **Privacy and Security Incident and Breach Policy** to investigate the complaint or incident.

### 2.3 Resolution

- 2.3.1 After the investigation is complete, the HIPAA Privacy & Security Officer will provide a written response to the complainant which will include:
  - 2.3.1.1 Description of the investigation;
  - 2.3.1.2 Description of the results of the investigation; and
  - 2.3.1.3 Any corrective steps taken.

## 3. DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

## 4. ROLES & RESPONSIBILITIES

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

## 5. RELATED DOCUMENTS

Definitions
Complaint Form
Privacy and Security Incident Breach Policy

## 6. DOCUMENT VERSION HISTORY

Original: 08/2023
Revised: 07/2024
Reviewed: 01/2026