DETROIT AREA AGENCY ON AGING

Policy Number/Policy Title: **1002/ PHI and HIPAA**	**Approved by:** **President & CEO** **Chief Compliance Officer & VP of Quality**	
Responsible Department: **Quality and Compliance**	**Applies to:** **All Departments**	
Effective Date: **3/1/2003**	**Last Date Revised:** **10/2025**	**Next Review Date:** **10/2026**

Policy Statement

The purpose of this policy is to describe DAAA's policy and procedures in ensuring that participant's protected health information (PHI), in accordance with DAAA's Notice of Privacy Practices (Notice), is not disclosed and in which circumstances a participant's PHI can be disclosed in accordance with HIPAA regulations.

The law requires us to keep our participants' PHI private. DAAA takes its participants' privacy seriously and expects DAAA employees, agents and business associates to do the same. DAAA has designated a Compliance Officer to manage and oversee the security procedures and processes put in place to ensure participants' PHI is kept private.

Definitions

HIPAA: Health Insurance Portability and Accountability Act of 1996. This Rule sets national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.

PHI: Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. Examples include:

- Names
- All geographical 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: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- 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
- Phone numbers or Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers, Health plan beneficiary numbers or Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Frequency of Policy Review

- Policies are reviewed and/or updated annually by the Management Team

Purpose / Scope

Minimum Necessary. In all cases in which we use or disclose a client's PHI, we must only do so to the minimum extent necessary to accomplish the underlying purpose of the use or disclosure. If you are unsure whether a use or disclosure meets this requirement, contact our Compliance Officer for clarification.

Uses and Disclosures. We may use or disclose PHI for treatment, payment, or health care operations (TPO). The following are some examples of permitted uses or disclosures:

- *Treatment.* A client's PHI may be used by or disclosed to any physicians or other health care providers involved with the health care services provided to that client.
- *Payment.* PHI may be used or disclosed in order to collect payment for the health care services provided to our clients.
- *Health Care Operations*. PHI may be used or disclosed as part of quality-of-care audits of staff and affiliates, conducting training programs, accreditation, certification, licensing, or credentialing activities.

Authorizations: If we have received written authorization from a client, we use or disclose PHI for any purpose consistent with that Authorization. We may not require such authorization as a condition of treatment or ability to receive services. A client may revoke an authorization at any time by writing to the Compliance Officer. However, such revocation will not affect any prior authorized uses or disclosures.

Family Members and Friends: With the client's permission, or in some emergencies, we may disclose PHI to family members, friends, or other people to aid in treatment, provisions of services or collection of payment. A disclosure of PHI may also be made if we determine if it is reasonably necessary or in the client's best interests for such purposes as allowing a person acting on the client's behalf to receive filled prescriptions, health care supplies, X rays, home and community-based services; etc.

Locating Responsible Parties: PHI may be disclosed in order to locate, identify or notify a family member, personal representative, or other person responsible for a client's care. A client may prohibit or restrict the extent or recipients of such disclosure, unless we determine in our reasonable professional judgment that a client is incapable of doing so. If we are so determined, we must limit the amount of PHI disclosed to the minimum necessary.

Disasters: We may use or disclose PHI to any public or private entity authorized by law or by its charter to assist in disaster relief efforts.

Required by Law: We must use or disclose health care information when we are required to do so by law. For example, PHI may be released when required by privacy laws, workers' compensation or similar laws, public health laws, court or administrative orders, subpoenas, certain discovery requests, or other laws, regulations or legal processes. Under certain circumstances, we may make limited disclosures of PHI directly to law enforcement officials or correctional institutions regarding an inmate, lawful detainee, suspect, fugitive, material witness, missing person, or a victim or suspected victim of abuse, neglect, domestic violence or other crimes. We may disclose PHI to the extent reasonably necessary to avert a serious threat to a client's health or safety or the health or safety of others. We may disclose PHI when necessary to assist law enforcement officials to capture a third party who has admitted to committing a crime against the client or who has escaped from lawful custody. If you are unsure of the lawful authority of the person requesting the PHI, contact the Compliance Officer prior to making any use or disclosure under this section.

Deceased Persons: We may disclose PHI of a deceased client to a coroner, health care examiner, funeral director, or organ procurement organization in limited circumstances.

Research: PHI may also be used or disclosed for research purposes only in those limited circumstances not requiring written authorization, such as those that have been approved by an institutional review board that has established procedures for ensuring the privacy of your PHI. Prior to conducting any research under this section, approval of our Compliance Officer must be obtained to ensure that all procedural requirements have been met.

Military and National Security: We may disclose to military authorities the health care information of Armed Forces personnel under certain circumstances. When required by law, we may disclose PHI for intelligence, counterintelligence, and other national security activities. Contact the Compliance Officer prior to making any use or disclosure of PHI under this section.

Fundraising: We may use demographic information and the dates of a client's health care to contact them for fundraising purposes. We may disclose this information to a business associate to assist us in fundraising activities. A client may opt out of receiving such information by notifying our Compliance Officer.

Access and Copies: In most cases, clients have the right to review or to purchase copies of their PHI by requesting access or copies in writing to our Compliance Officer. All such requests should be handled quickly and efficiently but should not interfere with our treatment of other clients. We require that a client call DAAA to review PHI at our office. Our Compliance Officer is responsible for setting copying fees.

Disclosure Accounting: We are required by law to maintain a Disclosure Accounting log of the instances, if any, in which PHI is disclosed for purposes other than those described in the following sections above: Use and Disclosures, Facility Directories, Family Members and Friends, Locating Responsible Parties, and Access and Copies. For each 12-month period, a client has the right, upon request, to receive one free copy of an accounting of certain details surrounding such disclosures that occurred after April 13, 2003. If a client requests a disclosure account more than once in a 12-month period, we will charge a fee for each additional request.

Additional Restrictions: A client may request that we place additional restrictions on our use or disclosure of PHI, but we are not required to honor such a request. We will be bound by such restrictions only if we agree to do so in writing signed by our Compliance Officer.

Amendments to PHI: A client has the right to request that we amend his or her PHI. Any such request must be in writing and contain a detailed explanation for the requested amendment. Under certain circumstances, we may deny the request but must provide you with a written explanation of the denial. A client has the right to send us a Statement of Disagreement, which we must file with the disputed PHI entry. We may then prepare and file a rebuttal to the client's Statement of Disagreement, a copy of which must be provided to the client at no cost. Please contact our Compliance Officer before changing or amending any health care record or other PHI.

Complaints: A client is entitled to file a complaint with DAAA or with the Secretary of the U.S. Department of Health and Human Services if he or she believes we have violated any Compliance rights with respect to our Notice of Privacy Practices. We shall not retaliate in any way if a client chooses to file such a complaint. All such complaints must be forwarded to the Compliance Officer.

CONFIDENTIALITY PROCEDURES

In-office Procedures.

- *Sign-in Sheets.* Public sign-in sheets should request only the client's name. Any other information collected from the client should be kept private.

- *Oral Communications.* Discussions about PHI should be held behind closed doors and/or out of earshot of those who have no right to access the PHI discussed.

- *Client Files.* All reasonable efforts must be used to prevent unauthorized people from accessing client files. Files should be monitored by staff to ensure they are accessed only by authorized personnel. Unattended files should be kept in a locked room or cabinet. Client files shall not be altered, copied or removed from the premises without first notifying the Compliance Officer.

- *Confidentiality Agreement.* Anyone with access to client records, files or other PHI must sign a confidentiality agreement. Violation of the confidentiality agreement should result in a reprimand, such as removal, demotion, suspension, or termination.

- *Fax Confidentiality*. PHI should be faxed only in emergencies. In all other cases, PHI should be sent by mail or hand delivery, marked "confidential." PHI should not be faxed on or to a machine that is accessible to the general public. Indicate the confidential nature of the fax on the cover sheet as well as each sheet of the document. The coversheet should also request that any erroneous recipient destroy or return the fax. Always notify the recipient of a forthcoming confidential fax and verify the fax number before faxing PHI. Wait to send the confidential fax until you are able to contact the recipient. Verify the fax number once again on the fax confirmation sheet after the fax is sent. If an error occurs, contact the accidental recipient and request the return or destruction of the fax.

- *Remote Consultation Confidentialit*y. Client Compliance and confidentiality must be maintained whenever PHI is viewed or discussed during a health care consultation session conducted over the telephone, Internet or similar remote communication device. The provider who is consulting must confirm that the consultation is attended only by individuals who have a legitimate interest in the client's care. Additionally, all PHI presented shall remain confidential.

- *Email Confidentiality*. PHI should not be sent by email or other electronic transmission unless it conforms to the appropriate encryption standard. The e-mail system and all messages generated or handled by e-mail, including backup copies, are property of DAAA. E-mail users have no right to Compliance in their use of the computer system, including e-mail. DAAA may monitor the content and usage of the computer system, including email, at any time and for any reason. E-mail Users should restrict use of the e-mail system to proper business purposes.

- *Electronic Data Confidentiality*. Officers, agents, employees, independent contractors, business associates and others using lab top computers or other electronic data media may not download, maintain, or transmit confidential client or other information without the written authorization of the Compliance Officer. Failure to comply with this provision may result in removal, demotion, suspension, or termination in some circumstances.