Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 19.05.01

Subject:	**Protected Health Information & HIPAA Compliance in Financial Documents**
Information Contact:	Office of Accounting Services Chief, (360) 664-5716
Authorizing Source:	**State Administrative & Accounting Manual (SAAM)** Chapter 5.10, About Data and Systems Access Chapter 20.20, Risk Assessment OCIO Policy 141 Executive Order 16-01, Privacy Protections and Transparency in State Government Information Security Standards Manual Information Security Procedures Manual
Effective Date:	January 18, 2019
Revised:	New
Approved By:	**Original signed by Judy Fitzgerald** Assistant Secretary/Chief Financial Officer Facilities, Finance, and Analytics Administration

Purpose

To identify the required control structures/safeguards for processing financial documents that contain protected health information (PHI) to ensure compliance with the health insurance portability and accountability act (HIPAA).

To establish procedures for processing financial documents that contain PHI to ensure compliance with HIPAA and protect against inappropriate disclosure of PHI.

Scope

This policy applies to all programs within department of social and health services (DSHS) that process payments and journal vouchers.

This policy does not apply to established client service payment systems (e.g. SSPS, ProviderOne and ACES).

Additional Guidance

DSHS Forms Picker

DSHS 03-420, OAS Enterprise Financial Systems Security Request

DSHS Administrative Policies

5.01, Privacy Policy

5.04, Records Retention

5.08, Physical Security Standards for Confidential Information and Financial Instruments

19.20.01, AFRS Security and Related Controls

15.10, Information and Technology Security

DSHS Privacy SharePoint Site

DSHS HIPAA Training

Definitions

Agency financial reporting system (AFRS) is the state of Washington's official accounting system.

A-19 invoice voucher is a form used by agencies to substantiate and authorize payment when a purchase order or field order (A17-A) is not involved and where vendor invoices are not used. This form is used to produce warrants using the agency financial reporting System (AFRS).

Client is a person who received services offered by the department based on their individual or family need.

Department refers to the department of social and health services (DSHS).

Disclosure is the release, transfer, or the providing of access to information outside of DSHS. (See Administrative Policy 5.01).

Electronic fund transfer (EFT) is any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument that is initiated through an electronic terminal, telephone instrument, computer, or magnetic tape to authorize a financial institution to debit or credit an account.

Headquarters fiscal program managers are principle fiscal contacts as listed on the facilities, finance, and analytics administration staff program assignment list, as posted on the office of accounting service's intranet under contact information.

Health information: Any information, whether oral or recorded, in any form or medium, that:

1. Is created or received by DSHS concerning a client or potential client;
2. Is related to the past, present, or future physical or mental health condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and
3. Identifies or can readily be associated with the identity of a client or potential client. "Health information" is considered the same as "health care information" in the health care information action (HCIA) (RCW 70.02.010). (DSHS Administrative Policy 5.01).

HIPAA is the health insurance portability and accountability act of 1996, 42 USC 1320d et seq. To implement HIPAA, the U.S. department of health and human services office for civil rights has adopted the HIPAA privacy rule, security rule and breach notification rules. (Administrative Policy 5.01)

Individually identifiable means that a record contains information, which reveals or can likely be associated with the identity of the person or persons to whom the record pertains, such as, names, addresses, client ID numbers, and unique characteristics. May also be known as individually identifiable health information or "IIHI." (DSHS Administrative Policy 5.01)

Program means the affected DSHS programs, including the division, office, or staff designated by the assistant secretary or division director as being responsible for compliance with this policy.

Protected health information (PHI) is individually identifiable health information about a client that is transmitted or maintained by a DSHS health care component in any form or medium. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe can be used to identify the individual. IIHI in DSHS records about an employee or others who are not clients is not PHI. See Administrative Policy 5.03 for provisions relating only to PHI of client. (DSHS Administrative Policy 5.01)

Vendor is any person, business, non-profit, or government entity who provides goods or services to DSHS or its clients. A vendor may or may not have a contractual agreement.

Regular warrant is a warrant produced through AFRS that is prepared by the program and is not automatically mailed out by central mail services. The warrant is returned to the issuing office and the issuing offices mails the warrant with additional supporting documentation.

Policy

A. Financial records must comply with HIPAA & PHI regulations.

The department must safeguard client PHI that is collected, used, and stored as required by HIPAA. PHI includes, but is not limited to the following identifiers:

1. Client names
2. SSN (last four digits)
3. Birthdates
4. Client ID
5. Email address
6. Client medical records
7. Mental health evaluations
8. Bank account number
9. Client status
10. Bills from health care providers

11. Information about health care services provided to a client
12. Information about the fact that the client has received treatment
13. Demographic information linked to health information about a client
14. Individually identifiable health information (IIHI).

IIHI must be removed from shared client data.

For more information on HIPAA, PHI and the complete list of individually identifiable health information identifiers, visit the DSHS privacy SharePoint site.

B. All financial documents that contain PHI must be maintained or stored in a secure location.

All financial batches that contain PHI must be processed with the unique batch type. The office of accounting services (OAS) will assign each program a unique batch type to use for processing financial documents that contain PHI. Use of the unique batch type ensures that backup documentation attached to payments and journal vouchers is only viewable in the management operations document imaging system (MODIS) to those that have access to the secure DSHS PHI accounting folder.

Headquarters FPMs must follow the procedures outlined in DSHS Administrative Policy 19.20.01 - AFRS security & related controls, to obtain or terminate staff access to their program's unique batch type for financial documents that contain PHI.

Headquarters FPMs must contact the technology services division (TSD) help desk to request or terminate staff access to the secure DSHS PHI accounting folder in MODIS.

For programs that use MODIS to retain financial documents, imaging the documents into the secure DSHS PHI accounting folder in MODIS is a technical safeguard to help ensure that only authorized staff will have access to financial documents that contain PHI. Access to this folder should be limited to individuals identified by the headquarters FPMs due to the confidential information.

The department will perform a biennial review (once every biennium) of staff access to the secure DSHS PHI accounting folder in MODIS. The headquarters FPMs will conduct this biennial review in conjunction with the biennial review of AFRS access. They will review the list of individuals who have access to the secure folder in MODIS. If any individual no longer needs access, the headquarters FPMs will contact the TSD help desk to remove that person's access.

For more information on conducting the biennial review of AFRS access, see DSHS Administrative Policy 19.20.01 - AFRS security & related controls.

Programs that retain paper copies of financial documents, and that do not image payment batches into MODIS, must ensure the batches including the remittance advice and supporting documentation are stored in a secure location with limited access. For

additional guidance, see DSHS Administrative Policy 5.08 - DSHS minimum physical security standards for confidential information and financial instruments.

C. Information that is entered in AFRS cannot contain PHI

Programs must:

1. Ensure that no PHI information is entered into AFRS. This includes ensuring no PHI information shows on the remittance advice or enterprise reporting. If information is entered in the following AFRS fields that information will be reflected on the remittance advice and enterprise reporting:
   a. Invoice number
   b. Account number
   c. Vendor message
   d. Agreement number
   e. Provider number

2. If the vendor requires the client's name or other PHI to apply the payment, the payment must not be made by EFT or inserted warrant. The payment must be made using a regular warrant and the PHI information attached to the warrant prior to the payment being mailed.

Procedures

A. To ensure that no PHI Information is entered into AFRS, program staff must ensure the following:

1. When making a payment with inserted warrant or EFT, ensure no PHI is included in the fields noted in policy point C.1.

2. When making payment using a regular warrant and PHI information must be sent to the payee, the warrant must be returned to the issuing office. The issuing office must:
   a. Attach a copy of the invoice and the remittance advice with the payment.
   b. Mail the warrant with the remittance advice and supporting documentation.
   c. If the program images payment batches, send to MODIS for imaging, including the supporting documents.
   d. If the program does not image payment batches, the invoice and the supporting documentation must be stored in a secure location with limited access.
   e. Journal vouchers that do not contain PHI information must be placed into MODIS but not into the secure folder. Only journal vouchers with PHI information must be placed into the secure DSHS PHI accounting folder in MODIS.

B. Conducting biennial review of staff access to a secure folder in MODIS

1. Biennial review- (Performed in April every even year)

OAS must:

a. Request current list of employees with access to the secure DSHS PHI accounting folder in MODIS from the TSD help desk.
b. Forward the lists to the appropriate headquarters FPMs for the biennial review.

TSD must:

a. Provide current list of employees with access to the secure DSHS PHI accounting folder in MODIS to OAS, as requested.

Headquarters FPMs must:

a. Review the list of individuals who have access to the secure DSHS PHI Accounting folder in MODIS.
b. Email the TSD help desk requesting the employee's access to the secure DSHS PHI accounting folder be terminated if any individual no longer needs access.