HIPAA Privacy Safeguards	
POLICY #124	Page 1 of 7
Effective Date: 4/25/2023 **Prior Version Date(s):**	Approved 4/25/2023 – Josette Manning, Cabinet Secretary

1. Policy Purpose

The purpose of this policy is to establish privacy safeguards that protect individually identifiable health information (IIHI) from unauthorized use or disclosure and to further protect such information from tampering, loss, alteration, or damage. Individually identifiable health information (IIHI), also known as protected health information (PHI), is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
- relates to the past, present or future physical or mental health or conditions of an individual; the provision of healthcare to an individual; and that
    - identifies the individual; or
    - there is a reasonable basis to believe the information can be used to identify the individual. (45 C.F.R. § 160.103).

It is intended for this policy to work in conjunction with other policies of the Department of Services for Children, Youth, and Their Families (DSCYF) and the Department of Technology and Information (DTI) which have additional safeguards for protecting data containing IIHI.

2. Scope

DSCYF complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Privacy Rule requires covered health care components to implement appropriate administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of IIHI. Agencies are not asked to "guarantee" the safety of IIHI against all imaginable assaults; instead, agencies are instructed to use protections that are flexible, scalable, and provide reasonable safeguards.

Safeguards addressed in this policy include administrative, physical, and technical protections necessary for safeguarding IIHI as it is found in the working environment (e.g., oral communications, paper records, computer screens, etc.).

3. Policy / Procedures

Administrative Safeguards

DSCYF staff shall safeguard IIHI that is generated, received, and maintained throughout the agency. Confidential information that is transmitted by facsimile (fax) machines, e-mail, printers, copiers, and by telephone or other oral means of communications shall be protected from unauthorized use and disclosure.

To safeguard disclosure of IIHI, when required for a business need, staff shall confirm the following prior to disclosure:

1. the disclosure is authorized by the client,
2. the disclosure does not violate any restrictions on disclosure that the client has requested, and the agency has granted per the procedure outlined in DSCYF Policy 205 (Confidentiality of Client Records), or
3. the disclosure is required or permitted by law.

DSCYF internal mail or hand delivery

All documents containing IIHI shall be placed in a secure container (e.g., sealed envelope, secured box) that is labeled "Confidential," addressed to the recipient, and includes a return name and address. Documents that are hand delivered must be delivered by courier service or a department staff member.

Facsimile or E-Facsimile

Incoming fax transmissions of documents that contain IIHI must be protected from unauthorized disclosure to staff or others who are not authorized to access the information.

1. Prior to receiving such documents, agency staff shall attempt to schedule the transmission with the recipient so that the faxed document can be promptly retrieved by staff. E-faxing is preferred when available.

2. In addition, incoming fax cover sheets should contain the:
   a. sender's name, mailing address, e-mail address, telephone number, and fax number
   b. recipient's name, telephone number, and fax number
   c. number of pages transmitted, including coversheet

3. Divisions should notify routine recipients of faxed documents containing IIHI immediately if their fax number(s) change, so that the recipient's records and pre-programmed numbers can be updated accordingly.

4. In the event a misdirected fax is received, the recipient should contact the sender immediately and shall destroy the information by shredding the document.

Efforts to protect outgoing fax transmission of documents containing IIHI shall be initiated by staff as listed below:

1. All outgoing faxes shall include a cover sheet that contains a confidentiality statement like the following example:

   **** Fax Confidentiality Notice**** This message and any attachment(s) are confidential. This fax is only for the use of the intended recipient(s). If you are not the intended recipient of this fax you are hereby notified that any disclosure, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this fax in error, please notify the sender immediately and then destroy this fax and any attachment(s). Thank you.

2. In addition to the required confidentiality statement, fax cover sheets should contain the:
   a. sender's name, mailing address, e-mail address, telephone number, and fax number
   b. recipient's name, telephone number, and fax number
   c. number of pages transmitted, including coversheet

3. Prior to faxing such documents, agency staff shall attempt to schedule the transmission with the recipient so that the faxed document can be promptly retrieved by the recipient. E-faxing is preferred when available.

4. Divisions should request that routine recipients of faxed documents containing IIHI inform the divisions immediately if their fax number(s) change, so that agency records and pre-programmed numbers can be updated accordingly.

5. Staff authorized to send faxes with IIHI shall check the recipient's fax number before transmittal and shall confirm delivery via telephone or review of the confirmation sheet of fax transmittal.

6. In the event of a misdirected fax, the recipient should be contacted immediately and shall be asked to destroy the information by shredding the document. Misdirected faxes are considered accidental disclosures.

E-mail

1. Only transmit e-mails containing IIHI when required for a business need.
2. Only transmit e-mails containing IIHI, to business associates or to other covered entities.
3. Avoid including IIHI in the subject line or body of an e-mail (for example, use an individual’s initials or PID number instead of their full name).
4. If it is essential for the efficiency of business operations to send IIHI via e-mail, the information should be sent by encrypted e-mail.

5. Include the least amount of identifying information possible in both the body and attachment(s). This doesn't restrict the inclusion of identifying information when necessary.
6. Ensure that e-mails are addressed correctly by reviewing the recipient's e-mail address before sending the e-mail, to ensure the e-mail software did not automatically fill-in an incorrect e-mail address after the first few characters of the address were typed.
7. In the event of a misdirected e-mail with a file attachment that contains IIHI, the staff shall immediately attempt to recall the e-mail. If the recall is unsuccessful, staff shall remove the unintended recipient's access to the e-mail through the encryption software. Once access has been removed, staff shall immediately contact the recipient and ask them to delete the e-mail and attachment. Misdirected e-mails are considered accidental disclosures.
8. If the recipient is unable to access the encrypted email, staff should contact the recipient to determine another secure method of delivery such as sending a password-protected document.
9. A confidentiality statement like the following example shall be included on all e-mails containing IIHI in the email narrative or as file attachments:

Example: **** E-mail Confidentiality Notice**** This electronic message and any attachment(s) are confidential. This e-mail is only for the use of the intended recipient(s). If you are not the intended recipient of this e-mail message you are hereby notified that any disclosure, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately by replying to this e-mail and then delete this message and any attachment(s) from your system. Thank you.

Telephone

Whenever it is necessary for agency staff to discuss IIHI via the telephone with a client or a client's family members, agency workforce members, business associates, or other providers, staff must adhere to the following requirements for protecting such information.

1. When receiving incoming calls, staff shall not discuss IIHI until all the following can be confirmed:
   a. the identity of the caller (verifying the number on the caller ID, recognizing the voice of a case participant who has consent to receive information, etc.),
   b. the caller has a need to know,
   c. the use or disclosure of confidential information is permissible.

   If confirmation cannot be made, the agency shall neither confirm nor deny the client has historically or is currently receiving services from the agency. The worker can ask for the request to be provided in writing (utilizing an authorization to release

information if appropriate) so that the person's identity and need to know can be verified before providing the information.

2. When making outgoing calls, staff shall:
   a. not discuss IIHI until the identity of the person on the phone line has been confirmed.
   b. leave a message requesting the person they need to speak to return the call if an answering machine or voice mail system picks up the call.
   c. ONLY include the name and telephone number of the person that should receive the return call in messages (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313").
   d. not include confidential health information in messages left on an automatic answering machine or voicemail system.

Technical Safeguards

DSCYF shall safeguard IIHI that is generated, received, and maintained throughout each division in their computer systems and other electronic media.

Each division shall determine which staff, based on job responsibility, require access to IIHI in electronic data. Privileges shall be established on a "need to know" basis for each user relative to their specific relationship with clients and specified business needs for accessing IIHI. It will be the responsibility of each division to determine the level of IIHI a staff member can access, such as an entire record, department files, child and family files, software applications, electronic data, electronic report files, etc. The IIHI access level granted to an individual shall be the minimum necessary for the staff member to perform the essential functions of their position. Unique user identifiers and passwords shall be used to monitor and control access.

Physical Safeguards

DSCYF shall safeguard IIHI that is generated, received, and maintained throughout each agency by establishing protections used for equipment, supplies, records, and work areas; to prevent unauthorized use or disclosure of IIHI maintained by the agency.

Divisions must ensure these areas are routinely manned or physically secured as appropriate during business and non-business hours and that such areas are accessed only by authorized staff. Securing confidential information may be as simple as locking file cabinets, safes, and desk drawers or as complex as relocating an entire work area to a more secure location.

Divisions shall ensure that observable IIHI displayed on computer screens is adequately shielded from unauthorized disclosure. Divisions shall safeguard IIHI displayed on computer monitors by:

1. positioning computer monitors so that only authorized staff may view it
2. clearing information from the computer screen when it is not being used by closing the file or program or activating a password-protected screen saver.

Each division shall take reasonable steps to ensure the privacy of client information in open areas where visitors, vendors, or the public are permitted. General safeguards shall include measures the sites have implemented that protect IIHI from unauthorized use or disclosure.

Site safeguards include the following:

1. Sign-in sheets - Ensure sign-in sheets that are viewed by multiple people do not contain health information and unnecessary identification information
2. Client and staff conversations - establish precautions to prevent conversations regarding client information from being overheard by others. Designate an area away from waiting areas to have conversations involving confidential information.
3. Intercom - limit information given over an intercom system.
4. Client records - assure client records used in staff areas are reasonably protected to prevent inadvertent disclosures. For example, place a cover sheet over records sitting on a desk or position a client's record so that the client's name is not visible. Maintain client records in secure area. (e.g., locked file cabinet).

Visitor safeguards should include:

1. Sign-in logs - ensure sign-in logs are used that record the visitor's name, company, area visited, time in, and time out.
2. Badges - provide visitors with identification badges where available.
3. Escort - establish procedures for when visitors must be escorted within the site. Unescorted visitor access should be limited to those areas that do not contain IIHI.

Each division shall establish a process for safely disposing of paper and other materials containing IIHI. It is recommended that, where practical and when permitted, paper materials containing IIHI be shredded. All steps in the shredding process shall be protected, including storage and handling of any shred boxes, bins, and bags containing IIHI to be destroyed.

Allowing DSCYF workforce members to remove IIHI from a premises for purposes other than treatment, investigation, or in response to a court order or allowing workforce members to access IIHI outside of the secured work environment, is strongly discouraged. However, it is recognized that there may be circumstances where work outside of the secured environment is necessary. DSCYF divisions shall develop and implement procedures to ensure the security of confidential information taken outside the secured work environment, including, but not limited to, the following guidelines.

1. Ensure privacy and security of remote work area,
2. Restrict telephone conversations to a private area,
3. Ensure faxed documents are handled according to the guidelines in this policy, and

4. Secure confidential information in locked rooms or locking storage containers (e.g., filing cabinets, desk drawers) when not in use.

Employees with an approved telework alternative work arrangement must abide by security measures contained within this policy and DSCYF Policy #306: Alternative Work Arrangements.

4. Legal Authority / Associated Regulations/Requirements

45 C.F.R. § 160.103
Health Insurance Portability and Accountability Act of 1996 - Public Law 104-191
DSCYF Policy #306 Alternative Work Arrangements

5. Responsibility for this Policy

The Department Privacy Officer is responsible for providing guidance regarding this policy.