Policy Overview

Utah Department of Health & Human Services

Date: 01/05/2023
Policy: 70.04.04- HIPAA Administrative, Technical, and Physical Safeguards Pertaining to Protected Health Information
Vote Needed: Yes

Policy Summary: This policy discusses the importance of protecting private information within the guidelines of HIPAA and USDC procedures. It breaks down procedure of safeguarding PHI by paper, electronic, oral, and visual representations. It also discusses limits to smartphones or other mobile data devices as well as social media usage.

Important Changes/Updates: Overall new formatting to meet new DHHS form/graphic standards, defining PHI, removing specific names/contact numbers, adding information about two factor authentication, adding social media posting guidelines, and removing redundant information.

Reasoning and/or Benefits: By reformatting, removing specific names/contact numbers, and removing redundant information, USDC is following new DHHS best practice recommendations. By not naming specific individuals and listing numbers, policies are able to remain intact when staff leave positions or numbers change. Removing redundant information makes policies much easier to read and follow for staff.

Defining PHI establishes just how much information the term PHI covers and shows how important it is to have safeguards in place.

There is a need to update information about two factor authentication as new safety guidelines are given from DTS.

It is important to add social media/posting specifics since phones are everywhere are our staff continues to skew younger.

UTAH STATE DEVELOPMENTAL CENTER POLICY AND PROCEDURES	
Policy: 70.04.04	Page 1 of 6
HIPAA Administrative, Technical, and Physical Safeguards Pertaining to Protected Health Information	
Reviewing Entity: HIPAA Committee ***Related Policies, Applicable Standards, Statutes****: Health Insurance Portability & Accountability Act of 1996 (HIPAA), 45 CFR 164.530 and Health Information Technology for Economic and Clinical Health Act (HITECH). See American Recovery and Reinvestment Act of 2009, 13400 (PL 111-115); 45 CFR 164.400-164.414.*	

Original Effective: 04/14/2003	Revision: 11/03/2022	Next Review Due: 11/2025

I. DESCRIPTION

USDC acquires, creates, accesses, uses, discloses, transmits, maintains, and destroys protected health information in accordance with HIPAA, HITECH, and the Omnibus Rule.

II. DEFINITIONS

The following terms are defined for this policy as:

A. **USDC:** Utah State Developmental Center
B. **HIPAA**: Health Insurance Portability and Accountability Act of 1996
C. **HITECH**: Health Information Technology for Economic and Clinical Health Act
D. **PHI**: Personal Health Information: any individually identifiable health information collected from an individual, whether oral or recorded in any form. PHI encompasses information that identifies an individual or might reasonably be used to identify an individual. Information is deemed to identify an individual if it includes either the individual's name or any other information that taken together or used with other information could enable someone to determine an individual's identity. (Examples: date of birth, medical records number, health plan beneficiary numbers, address, zip code, phone number, email address, fax number, IP address, license numbers, full face photographic images or social security number)
E. **PIN**: Personal Identification Number
F. **DHRM**: Division of Human Resource Management

G. **DHHS**: Department of Health and Human Services

III. POLICY

A. Establish appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
    1. USDC shall take steps to safeguard PHI from any intentional or unintentional use or disclosure that is in violation of HIPAA and USDC privacy policies. Safeguarded information may be in any medium including paper, electronic, oral, and visual representations of confidential information.
    2. USDC shall conduct accurate and thorough assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity or business associate.

IV. PROCEDURE

A. Safeguarding PHI
    1. Paper
        a) Each USDC workplace shall store files and documents containing PHI in locked rooms or storage systems.
        b) In workplaces where lockable storage is not available, USDC staff shall make reasonable efforts to ensure the safeguarding of PHI.
        c) Each USDC workplace shall ensure that files and documents awaiting disposal or destruction in desk site containers, storage rooms, or centralized waste/shred bins are appropriately labeled, disposed of on a regular basis, and have measures in place to minimize access.
        d) Each USDC workplace shall ensure shredding of files and documents is performed on a timely basis, consistent with record retention requirements.
        e) Patient records shall not be removed from the premises except when required for treatment, payment, healthcare operations, or when authorized by law.
            1) If records are required to be removed from the premises, safeguards shall be in place to maintain privacy and confidentiality, including, but to limited to, being kept under lock and key in a restricted area.
            2) Patient records shall not be stored in a vehicle without a custodian under any circumstances.
            3) Any lost or misplaced records shall be immediately reported to the privacy officer.
        f) All documentation shall be sent to the medical records department for proper management, storage, retention, and destruction.

g) No PHI shall remain in any area, other than medical records, 45 days post discharge of an individual.

2. Electronic
    a) Staff are responsible for all entries and queries performed under their unique computer identity.
    b) Remote access may be granted to select individuals who have a verified business necessity.
        1) Individuals requesting remote access shall complete a remote access request form, which will be reviewed and approved by the USDC steering team.
        2) The signed form will be electronically filed by a designated IT staff member.
    c) PINs for electronic signatures are obtained by signing an access and confidentiality agreement.
        1) The signed agreement shall be filed in the medical records department in the electronic record system.
        2) PINs shall not be shared or used by any other individual.
    d) Computer workstations shall have a screen saver password in place.
        1) Staff shall not leave their computers unattended without initiating the system lockout or signing off.
        2) E-chart shall automatically lock out the user when no activity is detected for ten minutes.
    e) Computers shall be accessed with two factor authentication, including using a physical token in the possession of the user.
        1) Staff shall register their token to their username.
        2) Staff shall only use their physical token to access computer systems under their own unique login, password, or PIN. Sharing the token with other staff is strictly prohibited.
        3) Staff shall have the token in their possession at all times.
        4) Staff shall notify the switchboard or building coordinators as soon as possible if they lose or misplace their physical token.
        5) Staff shall return the physical token to the building coordinator, switchboard, or human resources upon separation from USDC.
    f) When individual information is added electronically through notes, comments, or text field in e-Chart, first name and last initial and file number are the only identifiers to be included.
    g) When individual information is included in email correspondence, first name, last initial, and file number shall be the only identifiers used.

h) Audits of access to electronic records shall be conducted at least biannually. In addition, random audits based on unique circumstances shall be conducted:
    1) When questionable access is detected.
    2) If access is determined to be inappropriate.
        a. Requests for explanation shall be sent to the staff and their supervisor for follow-up.
        b. Appropriate action shall be taken following DHRM and DHHS rules with responses sent to the privacy officer.
i) Electronic communications between legally authorized persons and USDC may opt in to encrypted electronic communications.
    1) If a legally authorized person chooses encrypted emails as a preferred method of communication, a verification email will be sent to the email address provided. The preferred method of communication may be changed at any time.
    2) To ensure continuity and privacy, USDC medical records shall be notified as soon as possible if there is a change to a legally authorized person's email address.
j) Electronic recording devices, audio or video, such as cameras, camera phones, mini-cams, tape recorders, personal digital assistants, etc. shall not be used by any person for the recording of individuals without prior written HIPAA compliant authorization.
    1) Authorization is not required for USDC surveillance cameras.
k) An individual may give informed consent for videotaping, photographing, or recording by completing an authorization form. The recording may only be used for the stated purpose.
l) USDC security or nursing may take digital photos of an individual when there has been an injury.
m) All recordings which are not specifically authorized to be disclosed outside of USDC shall be sent to the medical records department for proper management, storage, retention, and destruction.
    1) There shall be no PHI remaining in any area, other than medical records, 45 days post discharge of an individual.
n) If a request for an interview or recording by the media is received, the public information officer for DHHS shall be notified.
    1) Individual authorization shall be obtained by completing the USDC media authorization form prior to any disclosure.
o) Electronic storage devices containing PHI shall be encrypted and not taken off USDC grounds unless specifically authorized.
    1) Electronic storage devices that contain, or ever have contained, PHI shall be sent to the medical records

department for proper management, storage, retention, and destruction.

2) No PHI shall be saved to any type of removable media, i.e. jump drives, disks, thumb drives, etc.

3. Oral
    a) USDC staff shall take steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs.
        1) Discussions and gatherings, including meetings, shall be held in areas that cannot be heard by others. Incidental uses or disclosures of PHI may occur when discussions are overheard. Such incidental uses or disclosures are not considered a violation provided that reasonable safeguards are utilized and USDC complies with the minimum necessary requirements, where applicable.
    b) Individual information shall only be discussed with authorized individuals for authorized purposes.
        1) Discussions shall not be held where other individuals, staff, or visitors not directly involved in care may be overheard.
    c) Precautions shall be taken by staff to use personal cell phones away from treatment areas.
    d) Each USDC workplace shall foster workforce awareness of the potential for inadvertent verbal disclosure of PHI.
4. Visual
    a) USDC shall ensure PHI is shielded from unauthorized disclosure on computer screens, information boards, and paper documents.
    b) Individual's first name and last initial may be written on communication boards inside the individual's bedroom and apartment to clarify appointments or on a picture of the individual or a piece of artwork the individual has created.

B. USDC limits the use of smartphones and other mobile data devices that create, store, access, transmit, or receive emails via the State of Utah system whether USDC issued or personal. Smartphones and other mobile data devices that are used via the State of Utah system shall meet the following criteria:
    1. Install mobile device management software on the device prior to connecting to state systems.
    2. The user shall use a password to access the mobile device and have encryption software enabled.
    3. Software shall be kept up to date. The user shall use the most recent operating system available for the mobile data device and the user shall apply security updates for any other software in a regular and timely manner unless instructed otherwise by USDC.

C. USDC prohibits staff from posting any individual related PHI, even if the individual is not named or identified, on social media sites whether at work or on personal time.
    1. USDC staff are not allowed to discuss individual-related information on blogs, social media, and other internet platforms.
    2. Posting stories or pictures about nameless individuals is also prohibited.
    3. USDC staff are obligated to notify their supervisor and the privacy officer if they come across anything on social media sites that is a suspected breach of confidentiality.
    4. Written PHI authorization shall be obtained from the guardian or self-guardian prior to communication with an individual and a staff member on any social media, blogs, or internet platform. Staff shall receive consent from the individual's treatment team after review and consideration prior to communication. Any communications between an approved staff and an individual will not be further disseminated, posted, or shared.
    5. An inventory of mobile data devices owned by USDC shall be maintained in the business office.

D. USDC shall put administrative safeguards in place for PHI. USDC shall identify the staff or classes or staff who need access to PHI to carry out their duties.
    1. For each person or class of persons, supervisors will identify the categories of PHI to which access is needed, and identify any conditions appropriate to the access.
    2. USDC shall conduct periodic and random reviews of the effectiveness of the administrative safeguards.
    3. All USDC staff shall be required to read and sign the access and confidentiality agreement form before obtaining computer access.
        a) This form is filed in the staff's personnel file in the human resource office.

E. USDC staff shall report all suspected intention or accidental violations of privacy policies and procedures to the privacy officer.

F. When staff terminates, the supervisor shall notify the Help Desk to disable computer access. The supervisor will additionally notify the switchboard to disable the terminating staff's identification badge.

V. EXCEPTIONS

A. The superintendent may make exceptions to this policy as allowed.

_____

Timothy Mathews
USDC Superintendent