Policy Overview

Utah Department of Health & Human Services

Date: 01/05/2023

Policy: 70.08.02- HIPAA Safeguards Pertaining to Protected Health Information for iPads

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 for newly implemented iPads. The iPads are still in a pilot program and have not been implemented across campus yet. As more staff are able to use iPads, and new issues/questions arise, updates will be made to this policy. The policy addresses use of electronic PHI and social media.

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 noting iPads cannot be used away from USDC campus.

Reasoning and/or Benefits: By reformatting and removing specific names/contact numbers, 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.

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 iPads are able to access the internet when in use.

UTAH STATE DEVELOPMENTAL CENTER POLICY AND PROCEDURES	
Policy: 70.08.02	Page 1 of 3
HIPAA Safeguards Pertaining to Protected Health Information for iPads	
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: 11/03/2022	**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. **DHHS:** Department of Health and Human Services
F. **PIN:** Personal Identification Number
G. **MFA:** Multi-Factor Authentication

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. USDC workplace practices safeguarding PHI for iPads
    1. Electronic
        a) Staff are responsible for all entries and queries performed under their unique user identification.
        b) Staff shall obtain system access and login as specified in technology services policy and procedure.
        c) iPads will have a shared user PIN to open the iPad.
            1) Staff shall not leave any iPad unattended without pressing the home button which will initiate signing off the iPad.
            2) iPads shall be set to automatically lock out users when no activity is detected for five minutes.
            3) iPads shall be programmed to lock down and not work for any reason if removed from USDC campus.
        d) Apps on the iPad shall be accessed by logging into Utah ID using MFA which could be a physical token or an approved MFA app.
            1) Staff shall be given a MFA token or approved MFA app for their use while employed.
            2) Staff shall only use their MFA token or approved MFA app to access iPads under their own unique login, password, or PIN. Sharing the MFA token or app with other staff is strictly prohibited.
            3) Staff shall keep the MFA token or app in their possession at all times.
            4) Staff shall notify the switchboard or building coordinator immediately if their MFA token or app is lost or misplaced.

5) Staff shall return their MFA token to the switchboard, building coordinator, or human resources, or delete the approved MFA app from their device, upon separation from USDC.

2. Social Media
    a) 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.
    b) USDC staff are not allowed to discuss individual related information on blogs, social media, or other internet platforms.
    c) Posting stories or pictures about nameless individuals is prohibited.
    d) 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.

V. EXCEPTIONS

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

_____

Timothy Mathews
USDC Superintendent