

UTAH STATE DEVELOPMENTAL CENTER POLICY AND PROCEDURE MANUAL		
HIPAA ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS PERTAINING TO PROTECTED HEALTH INFORMATION		PAGE 1 OF 3
DIRECTIVE: 70.04	EFFECTIVE DATE: April 14, 2003	REVISION DATE: 9/20/2010
REVIEWING ENTITY: HIPAA COMMITTEE		
PURPOSE: The Utah State Developmental Center (USDC) will establish appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.		
AUTHORITY REFERENCE: HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996, 45 C.F.R. § 164.530 and “Health Information Technology for Economic for Clinical Health Act” (HITECH). See American Recovery and Reinvestment Act of 2009, § 13400 (P.L. 111-115); 45 CFR § 164.400 -164.414.		

Policy:

1. General

- a. USDC must take reasonable steps to safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral, and visual representations of confidential information (45 CFR 164.530).

2. Safeguarding protected health information - USDC workplace practices.

- a. Paper:
 - i. Each USDC workplace will store files and documents containing protected health information in locked rooms or storage systems.
 - ii. In workplaces where lockable storage is not available, USDC staff must make reasonable efforts to ensure the safeguarding of protected health information.
 - iii. Each USDC workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
 - iv. Each USDC workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.
 - v. Original patient records shall not be removed from the premises.
 - vi. All documentation must be sent to the must be sent to the Medical Records Department for proper management, storage, retention and destruction.
 - vii. There shall be no PHI remaining in any area other than Medical Records 45 days post discharge of patient.
- b. Electronic
 - i. Staff are responsible for all entries and queries performed under their unique computer identity.
 - ii. Individual's obtain system access and log in as specified in Technology Services policy and procedure.
 - 1. Remote access may be granted to select individuals.
 - a. Individuals desiring remote access must complete a Remote Access Request Form which will be reviewed and approved by USH Executive Staff.

- c. Oral:
 - i. USDC staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of protected health information, regardless of where the discussion occurs. **Exception:** In work environments structured with few offices or closed rooms, incidental uses or disclosures of protected health information 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 requirement where applicable. (45 CFR 164.502)
 - 1. Patient information may only be discussed with authorized individuals for authorized purposes
 - a. Discussions are not held where other patients, staff, or visitors not directly involved in patient's care can be overheard.
 - 2. Each USDC workplace must foster workforce awareness of the potential for inadvertent verbal disclosure of protected health information.
 - d. Visual:
 - i. USDC must ensure that protected health information is adequately shielded from unauthorized disclosure on computer screens, information boards, and paper documents.
3. **Safeguarding protected health information - USDC administrative safeguards.**
- a. USDC will identify the employees or classes of employees who need access to protected health information to carry out their duties.
 - i. For each person or class of persons, managers/supervisors will identify the categories of protected health information to which access is needed, and identify any conditions appropriate to the access.
 - b. USDC will conduct periodic reviews of the effectiveness of the administrative safeguards.
 - c. All members of the USDC workforce will be required read and sign the "Access and Confidentiality Agreement" form.
 - i. This form is filed in the individual's personnel file in the Human Resource Office
4. Members of the USDC workforce shall report all suspected intentional and/or accidental violations of privacy policies and procedures to the Privacy Officer.

Karen A. Clarke, Superintendent