

UTAH STATE DEVELOPMENTAL CENTER POLICY AND PROCEDURE MANUAL		
HIPAA ENFORCEMENT, SANCTIONS, AND PENALTIES FOR VIOLATION OF INDIVIDUAL PRIVACY RIGHTS		PAGE 1 OF 5
DIRECTIVE: 70.05	EFFECTIVE DATE: April 14, 2003	REVISION DATE: 9/20/2010
REVIEWING ENTITY: HIPAA COMMITTEE		
PURPOSE: The Utah State Developmental Center (USDC) will safeguard protected health information and minimize the risk of unauthorized access, use, or disclosure.		
AUTHORITY REFERENCE: HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996, 45 C.F.R. § 164.530 and "Health Information Technology for Economic and Clinical Health Act" (HITECH). See American Recovery and Reinvestment Act of 2009, section 13400 (P.L. 111-115); 45 CFR 164.400-164.414.		

Policy:

1. General.

- a. All members of the USDC workforce (employees, volunteers, interns, and others whose conduct is under the direct control of USDC) must guard against improper uses or disclosures of protected health information.
 - i. Members of the USDC workforce who are uncertain if a disclosure of protected health information is permitted are advised to consult with their privacy officer.

- b. All members of the workforce are required to be aware of their responsibilities under HIPAA and the USDC privacy policies.
 - i. All members of the workforce are required to participate in training and then to sign the "Access & Confidentiality Agreement" form, indicating they understand and agree to abide by HIPAA and the USDC privacy policies.
 - ii. USDC employees who violate HIPAA or the privacy policies are subject to corrective action or discipline consistent with the Utah State Department of Human Resource Management Rules, including but not limited to termination of employment
 - iii. Volunteers, interns, and others under the direct control of USDC who violate HIPAA or the privacy policies are subject to having their association with the USDC terminated.

- c. Any member of the USDC workforce who violates HIPAA may be personally subject to criminal prosecution and monetary penalties.

2. Definition of Breach

- a. A breach is an unauthorized acquisition, access, use, or disclosure of PHI, on or after September 23, 2009, which compromises the security or privacy of PHI; and poses a significant risk of financial, reputational, or other harm to the affected individual except when the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

**UTAH STATE DEVELOPMENTAL CENTER
POLICY AND PROCEDURE MANUAL**

**HIPAA ENFORCEMENT, SANCTIONS, AND PENALTIES FOR
VIOLATION OF INDIVIDUAL PRIVACY RIGHTS**

PAGE 2 OF 5

- b. A breach is not an unintentional, good faith acquisition, access, or use of PHI within the scope of employment if the PHI is not further acquired, accessed, used or disclosed by any person; or an inadvertent disclosure of PHI from a person authorized to access PHI to another person authorized to access PHI at the same facility when the PHI is not further acquired, accessed, used or disclosed without authorization

3. Breach Investigation

- a. Each breach and suspected breach shall be reported to the Privacy Officer as soon as it is discovered.
 - i. A breach of PHI shall be treated as “discovered” as of the first day of which such breach is known to the organization.
- b. The Privacy Officer shall investigate each suspected breach.
 - i. The investigation shall include a review of the information that was potentially breached, interviews with the patients and staff involved, gathering any additional information and supporting documents to determine whether a reportable breach occurred, and making recommendations to appropriate staff for any necessary response.
 - ii. The Privacy Officer shall make a preliminary determination of whether the circumstances of a breach pose a significant risk of financial, reputational, or other harm.
 - A. Based upon the findings of the preliminary determination, Executive Leadership will conduct a risk assessment to determine significance of financial, reputational or other harm.
- c. The Privacy Officer shall maintain a log of each suspected breach.
 - i. The log shall include a description of the information that may have been breached, the persons involved, whether the suspected breach is reportable , and the date of any required notifications.
- d. If the suspected breach is determined to not be a reportable breach but nevertheless violates HIPAA or these policies, it shall be referred to the breaching party’s supervisor or HR for corrective action, training, and further safeguards.
- e. Privacy Officer shall immediately consult with the Attorney General when a suspected breach may involve 500 or more individuals.

4. Notification of Breach

- a. The number of individuals affected by the breach determines when the notification must be submitted to the Secretary and to the patient or personal representative (45 CFR 164.408).
 - i. The patient, their personal representative, or next of kin (if patient is deceased) will be notified within 60 calendar days after the date of discovery.
 - A. Notification will be the same as it is to the patient or personal representative.

**UTAH STATE DEVELOPMENTAL CENTER
POLICY AND PROCEDURE MANUAL**

**HIPAA ENFORCEMENT, SANCTIONS, AND PENALTIES FOR
VIOLATION OF INDIVIDUAL PRIVACY RIGHTS**

PAGE 3 OF 5

- ii. Notification will be written in plain language, delivered first class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically and include:
 - A. A brief description of what happened, including the date of the breach, the date of the discovery of the breach, if known;
 - B. A description of the types of protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - C. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - D. A brief description of what USDC is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 - E. Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, Web site, or postal address.
- iii. In cases where there is insufficient or out-of-date contact information for individuals, then such substitute notice may be provided by an alternative following CFR 164.404.
- b. Notification of US Secretary of Health and Human Services
 - i. In addition to notifying affected individuals and the media (where appropriate), USDC must notify the Secretary of breaches of unsecured protected health information. USDC will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form.
 - A. If a breach affects 500 or more individuals, USDC must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, USDC may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. (45 CFR 164.408).
 - B. This notice must be submitted electronically by completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year.
 - C. If USDC has submitted a breach notification form to the Secretary discovers additional information to report, USDC

**UTAH STATE DEVELOPMENTAL CENTER
POLICY AND PROCEDURE MANUAL**

**HIPAA ENFORCEMENT, SANCTIONS, AND PENALTIES FOR
VIOLATION OF INDIVIDUAL PRIVACY RIGHTS**

PAGE 4 OF 5

may submit an additional form, checking the appropriate box to signal that it is an updated submission.

- c. Notification to Media
 - i. If a breach affecting more than 500 individuals, in addition to notifying the affected individuals, USDC is required to provide notice to prominent media outlets serving the State or jurisdiction.
 - ii. USDC will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.
 - iii. This media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.
 - d. Notification by a Business Associate
 - i. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify USDC following the discovery of the breach.
 - ii. To the extent possible, the business associate should provide USDC with the identification of each individual affected by the breach as well as any information required to be provided by USDC in its notification to affected individuals.
 - e. Administrative Requirements and Burden of Proof
 - i. USDC and business associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach.
5. **Retaliation prohibited.**
- a. No member of the USDC workforce will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:
 - i. Any individual for exercising any right established under the privacy policies, or for participating in any process established under the USDC privacy policies.
 - ii. Any individual for:
 - A. Filing a complaint with USDC or with the U.S. Department of Health & Human Service's Office of Civil Rights;
 - B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to privacy policy; or
 - C. Opposing any unlawful act or practice, provided that:
 - I. The individual has a good faith belief that the act or practice being opposed is unlawful; and
 - II. The manner of such opposition is reasonable and does not involve a disclosure of an individual's protected health information in violation of privacy policies.
6. **Disclosures by whistleblowers and workforce crime victims.**

**UTAH STATE DEVELOPMENTAL CENTER
POLICY AND PROCEDURE MANUAL**

**HIPAA ENFORCEMENT, SANCTIONS, AND PENALTIES FOR
VIOLATION OF INDIVIDUAL PRIVACY RIGHTS**

PAGE 5 OF 5

- a. A member of the USDC workforce or a USDC business associate may disclose an individual's protected health information and is not considered to have violated this policy if:
 - i. The USDC employee or business associate believes USDC has engaged in conduct that is unlawful or that otherwise violates professional/clinical standards or USDC policy, or that the care, services, or conditions provided by USDC could endanger USDC staff, persons in USDC's care, or the public;
and
 - ii. The disclosure is to:
 - A. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of USDC;
 - B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by USDC; or
 - C. An attorney retained by or on behalf of the USDC employee or business associate for the purpose of determining the legal options of the USDC employee or business associate with regard to this policy.

- b. A USDC employee may disclose limited protected health information about an individual to a law enforcement official if the employee is the victim of a criminal act and the disclosure is:
 - i. About the suspected perpetrator of the criminal act; and
 - ii. Limited to the following information about the suspected perpetrator:
 - A. Name and address;
 - B. Date and place of birth;
 - C. Social security number;
 - D. ABO blood type and rh factor;
 - E. Type of any injury;
 - F. Date and time of any treatment;
 - G. Date and time of death, if applicable; and
 - H. A description of distinguishing characteristics, including height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos.

Karen A. Clarke, Superintendent