POLICY INFORMATION

Document # **100**	Title: **HIPAA Privacy Regulations, Compliance & Definitions**	Print Date: **5/18/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Standard: **HIPAA**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 8/7/2016

I. POLICY STATEMENT

In accordance with 45 CFR § 160.103 and 164.501, CEHS adopts and implements this policy in order to:

1. Achieve and maintain compliance with the Standards for the Privacy of Individually Identifiable Health Information ("HIPAA or the "Privacy Regulations") promulgated by the U.S. Department of Health and Human Services ("HHS")
2. Provide definitions of the terms used in CEHS's HIPAA policies in accordance with the Privacy Regulations: and
3. Ensure that clinics and other entities that are part of the CEHS health care components notify the appropriate staff of any HIPAA complaints, potential violations and investigations.

II. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the health care component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

III. DEFINITIONS

The following terms and acronyms are used in the CEHS HIPAA privacy policies and have the following definitions and meanings; however, in the event that any definition below differs from the definition provided HIPAA, their definition shall govern:

Accounting of Disclosures - A written record of certain disclosures of PHI that may be required to be maintained and provided to a requesting individual under certain prescribed circumstances.

Authorization - A written document completed and signed by the individual that generally allows use and disclosure of PHI for purposes other than treatment, payment or health care operations.

Breach - The acquisition, access, use or disclosure of Protected Health Information in a manner which compromises the security or privacy of the PHI.

Business Associate/BA - A person, entity, company or organization that is not a member of USU's workforce and yet performs a function or activity on behalf of a health care component that involves the use or disclosure of PHI.

Business Associate Agreement/BAA - A contract between a HIPAA Covered Entity and a HIPAA business associate (BA). The contract protects personal health information (PHI) in accordance with HIPAA guidelines.

CEHS – Emma Eccles Jones College of Education and Human Services

Clinical Laboratory Improvement Amendments/CLIA - Federal legislation and the personnel and procedures established by it under the aegis of the Health Care Financing Administration (HCFA) for the surveillance and regulation of all clinical laboratory procedures in the United States.

Code of Federal Regulations/CFR - The codification of the general and permanent rules and regulations (sometimes called administrative law) published in the Federal Register by the executive departments and agencies of the federal government of the United States.

Common Rule - The Federal Policy for Protection of Human Subjects described in 45 CFR. part 46, Subpart A. The Common Rule provides protections for individuals and establishes the role of institutional review boards in achieving those protections.

Compliance Office - USU's Information Security Office oversees compliance for Utah State University.

Correctional Institution - Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a Sate or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders, adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity/CE - (1) a health plan; (2) a health clearinghouse; and/or (3) a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Covered Functions - Those functions of an entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse (that is, the function makes the entity a "Covered Entity" subject to HIPAA.).

Data Aggregation - With respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, means the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Data Breach - a use or disclosure of unsecured PHI as described in 45 CFR § 164.400 *et. Seq.*

Data Use Agreement/DUA - Establishes the permitted uses and disclosures of information by the recipient, consistent with the purposes of research, public health, or health care operations, limits who can use or receive the data, and requires the recipient to agree not to re-identify the data or contact the individuals.

De-Identified Information - Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. De-identified information is not subject to the HIPAA Privacy Rule.

Demographic Information - In context for the use and disclosure of PHI for fundraising purposes, demographic information generally includes the name, address and other contact information (such as phone numbers, e-mail addresses, etc.), age, gender, and insurance status

Designated Record Set/ DRS -

1. A group of records maintained by or for a covered entity that is:
    a. Medical records and billing records used by a covered entity to make decisions about an individual;
    b. The enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plan; or used, in whole or in part, by or for the plan to make decisions about individuals
2. For purposes of this definition, the term *record* means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.
3. The term *record* includes patient information originated by another health care provider and used by the covered entity to make decisions about the patient; and
4. The term *record* means tracings, photographs, videotapes, digital and other images that may be recorded to document care of the patient.

Direct Treatment Relationship - A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. (See "Indirect Treatment Relationship" definition.) Typically, a "face-to-face" or direct contact relationship.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

EHR - Electronic Health Record

EMR - Electronic Medical Record

Employer - As defined by the Internal Revenue Code, 26 U.S.C. 3401(d):

"(d) Employer: For purposes of this chapter, the term "employer" means the person for whom an individual performs or performed any service, of whatever nature, as the employee of such person, except that-

1) If the person for whom the individual performs or performed the services does not have control of the payment of the wages for such services, the term "employer: (except for purposes of subsection (a)) means the person having control of the payment of such wages, and
2) In the case of a person paying the wages on behalf of a nonresident alien individual, foreign partnership, or foreign corporation, not engaged in trade or business within the United States, the term "employer" (except for purposes of subsection (a)) means such person."

EKG - Electrocardiogram

Emancipated Minor - A person who is under 18 and is fully independent from their parents or guardian and has adult rights due to being married, a military member, or having been granted emancipation through a court order.

EPHI or ePHI - Electronic Protected Health Information

FDA - Food and Drug Administration

FERPA - Family Educational Rights and Privacy Act

Fundraising - The solicitation of funds to benefit the health care component. Permissible fundraising activities include appeals for money, sponsorship of events, etc. Fundraising does not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).

Health Care - Care, services, or supplies related to the health of an individual. *Health care* includes but is not limited to, the following:

1. Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service assessment, or procedure with respect to the physical or mental condition, or functional status, or an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health Care Clearinghouse - a public or private entity including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
2. Receives a standard transaction form another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Component (HCC) - Health care components are units within a hybrid entity. A HCC includes any component that would meet the definition of covered entity if that component was a separate legal entity. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations.

Health Care Operations - any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improved activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits and ceding, securing or placing a contract of health insurance for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR § 164.514. (g) are met, if applicable;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the entity; including but not limited to:
    a. Management activities relating to implementation of and compliance with the requirements of the HIPAA Privacy Regulations;
    b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed t such policy holder; plan sponsor, or customer.
    c. Resolution of internal grievances;
    d. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity and due diligence related to such activity; and

e. Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health Care Provider - A provider of services as defined by 45 CFR §160.103.

Health Maintenance Organization - as defined by 45 CFR §160.103.

Health Information - Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment of the provision of health care to an individual.

Health Oversight Agency - An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, or entities to who it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan - An individual or group plan that providers, or pays the cost of, medical care as defined at 45 CFR §160.103.

HHS - U.S. Department of Health and Human Services

HIPAA - Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et seq.*

HIPAA Privacy Regulations - The HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164.

HIPAA Privacy Rule - The HIPAA Privacy Regulations

HIM - Health Information Management

HIV - Human Immunodeficiency Virus

HR - Human Resources

Human Subjects Committee - USU's IRB and Privacy Board for HIPAA and research related issues. See http://rgs.usu.edu/rib for more information.

Hybrid Entity - Means a single legal entity: That is a covered entity; whose business activities include both covered and non-covered functions; and that designates Health Care Components (HCC) within an organization.

ID- Identification

Indirect Treatment Relationship - A relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual - The person, generally the patient, who is the subject of the PHI.

Individually Identifiable Health Information - Information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearing house; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate - A person incarcerated in or otherwise confined to a correctional institution.

Institutional Review Board/IRB - any board committee, or other group formally designated by and institution to review, to approve the initiation of, and to conduct periodic review or, biomedical research involving human subjects. The primary purpose of such review is to assure the protection of the rights and welfare of the human subjects.

Institutionally Related Foundation - a tax-exempt entity that collects funds for the health care component, has in its charter statement of charitable purposes an explicit linkage to the health care component, and channels collected funds to the health care component.

IP - Internet Protocol.

Joint Commission/JCAHO - Joint Commission on Accreditation of Healthcare Organizations.

Law Enforcement Official - An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set/LDS - Protected health information that excludes direct identifiers of individuals (patients), or of their relatives, employers, or household members. A limited data set is subject the HIPAA Privacy Rule and requires a Data Use Agreement prior to release of the data set for internal and external uses and disclosures. The elements of the LDS are set forth in 45 CFR §164.514

Marketing -

1. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
    a. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
    b. For treatment of the individual; or
    c. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or setting of care to the individual.

2. An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.
3. For examples of activities, arrangements or other communications that constitute marketing for this purpose, see HIPAA 114- Use and Disclosure of PHI for Marketing.

Mental Health Professional - includes only a physician who is licensed to practice medicine or osteopathic medicine, a licensed psychologist, a licensed registered professional nurse, a social worker, a licensed counselor, or a licensed marriage and family therapist.

Minimum Necessary - Only the minimum necessary PHI may be used or disclosed to achieve the intended purpose of the use or disclosure.

NCQA - National Committee for Quality Assurance

Notice/NPP - Notice of Privacy Practices

OCR - Office for Civil Rights, a sub agency of the U.S. Department of Health and Human Services authorized to investigate potential violations and enforce HIPAA's requirements. References to HHS in this or any other policy should be interpreted to include references to OCR.

Organized Health Care Arrangement/HCA -

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider
2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
    a. Hold themselves out to the public as participating in a joint arrangement; and
    b. Participate in joint activities that include at least one of the following:
        i. Utilization Review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
        ii. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or b a third party on their behalf; or
        iii. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A group health plan and a health insurance issuer or health maintenance organization (HMO) with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plan group health plans each of which are maintained by the same plan sponsor; or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMO's with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMO's that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Payment -

1. The activities undertaken by:
    a. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
    b. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
2. The activities in paragraph (1) of this definition related to the individual to whom health care is provided and include, but are not limited to:
    a. Determinations of eligibility of coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
    b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges;
e. Utilization review activities, including precertification and preauthorization
f. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    i. Name and address;
    ii. Date of birth;
    iii. Social Security Number;
    iv. Payment history;
    v. Account number; and
    vi. Name and address of health care provider and /or health plan.

Person - Those who may file a privacy complaint including the patient, individual, patient's personal representative, employee, business associate, group or organization.

Personal Representative - An adult who is authorized by law and by the individual to make decisions for a patient.

PHI - Protected Health Information

Privacy Board - (See Human Subjects Committee and IRB) A board that:

1. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
2. Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
3. Does not have any member participating in a review of any project in which the member has a conflict of interest.

Privacy Officer - See section IV.B

Protected Health Information - Individually identifiable health information that is maintained in any medium or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records covered by the Family Education Rights and Privacy Act (FERPA), and records held by a covered entity in its role as an employer.

Psychotherapy Notes - Notes recorded (in any medium) by a health care provider who is a mental health professional that:

1. Document or analyze the contents of conversation during a private counseling session or a group, joint or family counseling session, and
2. *Are separated from the rest of the individual's medical record*.

Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Psychotherapy notes are used only by the therapist who wrote them, maintained separately from the medical record and not normally involved in the documentation necessary for health care treatment, payment or health care operations.

Public Health Authority - An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of it official mandate.

Re-identified Information - Health information previously de-identified may be re-identified using a code, key or other record identifier. This re-identified information is PHI and is subject to the HIPAA Privacy Rule.

Required by Law - A mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law. *Required by law* includes, but is not limited to , court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statues or regulations that require the production of information, including statues or regulations that require such information if payment is sought under a government program providing public benefits.

Research - A systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge including;

1. Clinical Trial- A research study that includes treatment.
2. Health Services Research- A multidisciplinary field of inquiry, both basic and applied, that examines the use, cost, quality, accessibility, deliver, organization, financing, and outcomes of health care services to increase knowledge and understanding of the structure, processes, and effects of health services for individuals and populations, such projects apply scientific methods to test hypotheses and produce new, generalizable knowledge.

SSN or SS# - Social Security Number

State - Refers to one of the following:

1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

2. For all other purposes, *State* means any of the States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State Law - A constitution, statue, regulation, rule, common law, or other State action having the force and effect of law.

Transaction - The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Other transactions that HHS may prescribe by regulation.

Treatment - The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care provides relating to a patient, or the referral or a patient for health care from one health care provider to another.

URL - Universal Resource Locator

U.S.C. - United States Code

Use - With respect to individually identifiable health information, means the sharing, employment, application, utilization, examination, or analysis or such information within an entity that maintains such information.

Workforce Members - Employees, authorized volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes, for example, full-time, part-time, regularly scheduled contract workers, and members of the Board of Trustees.

IV. PROCDURES TO IMPLEMENT

Compliance with the HIPAA Privacy Regulations:

CEHS will:

1. Establish policies to achieve and maintain compliance with the HIPAA Privacy Regulations.
2. Comply with the following responsibilities in accordance with the Privacy Regulations:
    A. *Creation and Retention of Records* - Each HCC will timely create and maintain appropriate and accurate records as required by the Privacy Regulations and HHS. Each HCC will promptly provide copies of all such records to CEHS's Privacy Officer or his/her designee.
    B. *Notification of CEHS Privacy Officer or his/her designee* - Each HCC will immediately notify the CEHS Privacy Officer or his/her designee regarding:
        i. Potential HIPAA violations;
        ii. Complaints by any Individual or Person regarding potential HIPAA violations; and
        iii. Requests and demands from, and investigations by, HHS and OCR

3. Interpretation of Policies- University Conduct policies, Applicable State Law- These Policies are intended to be:
    A. Consistent with and subject to, the terms and provisions of the CEHS conduct policies; and
    B. Subject to the provisions of state law, these policies and procedures are to be interpreted in such a way that CEHS will comply with state law that is more protective of patient's privacy as well as state law that provides broader patient rights regarding patient information.

Privacy Officer and Security Officer:

1. *CEHS HIPAA Privacy Officer, "PO" and CEHS Security Officer "SO"*
    A. CEHS's Privacy Officer will provide guidance and recommendations regarding HIPAA compliance and the development and implementation of CEHS's HIPAA privacy policies and procedures, including the duties specified throughout.
    B. The CEHS Security Officer is responsible for the design of the CEHS privacy training and education program.
    C. The CEHS Privacy and Security Officers are responsible for the education and training of the CEHS workforce members.

2. *Clinic Privacy Officer ("CPO")*- The CPO (and, to the extent appropriate, designated directors or staff members) is responsible for the HCC's compliance with the HIPAA policies, including:
    A. Receiving privacy complaints;
    B. Answering questions from the workforce members, patients and others concerning HIPAA and the Notice of Privacy Practices;
    C. Monitoring compliance with the privacy policies;
    D. The CPO is responsible for ensuring that each HCC monitors it workforce members; activities for compliance with the privacy policies and take corrective actions when indicated;

E. Instituting investigations of alleged violations of the privacy policies, including responsibility to:
    i. To the extent practicable, correct or mitigate potential harm caused by any use/disclosure or PHI in violation of these policies;
    ii. Implementing corrective action with circumstances indicate;
    iii. Take reasonable actions to prevent continued and/or repeat violation of these policies; and
    iv. Document corrective actions and mitigation taken.

Implementation of Privacy Policies:

1. Each HIPAA privacy policy is part of and incorporated into CEHS's HIPAA policies and procedures.
2. Under the direction of the CEHS Privacy and Security Officers, each HCC will comply with the privacy policies and procedures.
3. The HIPAA privacy policies include:
    - USU-Hybrid Entity Declaration Policy: Designation of CEHS as a Hybrid Entity
    - HIPAA 100
    - HIPAA 101
    - HIPAA 102
    - HIPAA 103
    - HIPAA 104
    - HIPAA 105
    - HIPAA 106
    - HIPAA 107
    - HIPAA 108
    - HIPAA 109
    - HIPAA 110
    - HIPAA 111
    - HIPAA 112
    - HIPAA 113
    - HIPAA 114
    - HIPAA 115
    - HIPAA 116
    - HIPAA 117
    - Administrative 200
    - Administrative 201
    - HIPAA 202
    - HIPAA 203
    - HIPAA 204
    - Administrative 300
    - Administrative 400

- Administrative 500
- Administrative 600
- Administrative 700
- Administrative 800
- Administrative 900
- Administrative 1000
- Physical 2000
- Physical 3000
- Physical 4000
- Physical 5000
- Technical 6000
- Technical 7000
- Technical 8000
- Technical 9000
- Technical 10000

Workforce Education and Training -

1. All workforce members of CEHS's health care components will be educated and trained regarding the requirements of the Privacy Regulations and the CEHS privacy policies and procedures.
2. Education and training will take place promptly upon a workforce member's engagement with or employment by CEHS, and annually thereafter and/or whenever required by a change in the Privacy Regulations or CEHS's policies.
3. The Privacy and Security Officers will document the education and training provided and maintain records of the education and training for at least six years following the training.

Sanctions for Violations of Privacy Policies:

1. CEHS's policies and procedures relating to employee conduct and disciplinary action (**Policy 201- Sanctions**) describe or shall describe the types of behaviors that are counterproductive to the mission of CEHS and the provision of patient care. CEHS's policies relating to employee conduct and disciplinary action detail the potential sanctions that could be imposed in the event that an employee fails to comply with any policies, rules, practices, or reasonable expectations could lead to involuntary termination of employment. Any unauthorized use or disclosure of PHI, or failure to follow the CEHS privacy policies and procedures, including all HIPAA policies, may result in sanctions of workforce members
2. All sanctions applied to workforce members as a result of a violation or pattern of violations of CEHS's privacy policies and procedures will be documented in the workforce member's official personnel file.
3. Where CEHS knows of a material breach or violation of HIPAA by a Business Associate (including material violation of any term of the parties' Business Associate

Agreement/BAA), CEHS is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the BAA is not feasible, as determined by CHES, CHES will report the problem to HHS/OCR.

Mitigation:

1. CEHS must mitigate, to the extent practicable, any harmful effect that is known to CEHS of a use or disclosure of PHI in violation of its policies and procedures or the HIPA requirements by CEHS or CEHS's Business Associate.
2. When a member of the CEHS workforce has knowledge of a potential violation of HIPAA or these privacy policies or procedures, the workforce member must report the violation to the CPO, PO or SO. This obligation to report potential violations includes potential infractions committed by workforce members of any other covered entity, including members of any OHCA in which CEHS participates, as well as employees and agents of CEHS business associates.

Privacy Complaints:

1. Patients and other persons have the right to complain to CEHS and/or HHS if they believe privacy rights have been violated or CEHS has violated it privacy practices or HIPAA. Patients cannot be required to waive their rights to file a complaint with HHS, or their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
2. The Notice of Privacy Practices (**Policy 108 Notice of Privacy Practices)** must inform patients of their right to file a complaint with CEHS and HHS.
3. CEHS will receive, process and resolve complaints in a timely manner, document the resolution, and assure no retaliatory actions are taken against the person who files a complaint (including workforce members).
4. Privacy complaints received by a HCC will be reported to the Privacy & Security Officers and processed in accordance with CEHS.
5. CEHS will investigate:
    A. Privacy complaints about Business Associates, and
    B. Any substantiated and credible evidence of violations of privacy practices by a Business Associate. CEHS must act upon its knowledge of a violation as set forth in the policy.

Non-Retaliation –Complaints, Investigations and Opposition Exception:

CEHS and HCC will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient, workforce member, Business Associate or other person for:

1. Filing a complaint with HHS for violating the Privacy Regulations'
2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
3. Opposing any act or practice made unlawful by the Privacy Regulations, provided the individual or person has a good faith belief that the practice opposed n unlawful, and the

manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA regulation.

V. REFERENCES

CEHS Policy 108 - Notice of Privacy Practices

CEHS Policy 201 - Sanctions

The Federal Policy for Protection of Human Subjects (the "Common Rule"), 45 CFR Part 46

42 United States Code § *et seq.*

HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 CFR §160.103, 164.501, 164.504, 164.512, 164.514, 164.520, 164.530

Family Educational Rights and Privacy Act (FERPA)

USU Conduct Policies

VI. ATTACHMENTS

N/A