LEBANON COUNTY CAREER AND TECHNOLOGY C·E·N·T·E·R

Section: PROFESSIONAL EMPLOYEES

Title: PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (HIPAA)

Adopted: April 20, 2004

Revised:

	440. PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (HIPAA)	
1. Statement	It shall be the policy of the Lebanon County Career and Technology Center ("LCCTC") to protect and safeguard the protected health information ("PHI") collected, retained, maintained, used and disclosed consistent with the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") promulgated pursuant to The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Standards adopted by the Department of Health and Human Resources ("HHR"), any case law arising from the interpretation thereof, and any applicable state laws.	
2. Purpose	For purposes of this policy, all health information created and maintained by the LCCTC and its agents that is considered part of a student's "education record" under FERPA (Family Educational Rights and Privacy Act") is not subject to this policy. The LCCTC Joint Operating Committee and Administration recognize that, as an employer and health plan sponsor and provider of health care services, certain components within the organization engage in HIPAA-covered functions and must comply with the Privacy Rule; however, there are other components of the LCCTC that engage in non-covered functions and, thus, are not required to comply with the HIPAA Privacy Rule. Therefore, the LCCTC Joint Operating Committee hereby designates itself as a "Hybrid Entity" under HIPAA and its rules and regulations. The purpose of this policy is to identify and disseminate the framework and principles for information management that guide the actions and operations of the Plans in protecting, generating, and sharing individually identifiable health information collected, maintained, used and disclosed by the Plans.	
3. Definitions	Words and phrases used in this policy unless otherwise defined have the same meaning herein as in the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards" or the "Privacy Rule") found at 45 CFR Parts 160 and 164, as amended from time to time.	

PHI is Individually Identifiable Health Information (not to include information contained in an Educational Record protected by FERPA) created, maintained, or transmitted in any form or medium, such as written, electronic and oral communication by a covered entity. Individually Identifiable Health Information is information created or received by a health care provider, health plan, employer, or health care clearinghouse that identifies directly or reasonably could be used to identify an individual, living or deceased, and that related to the past, present, or future physical or mental health or condition of the individual, provision of health care to the individual, or payment for the provision of such health care.

4. Responsibility

The LCCTC Joint Operating Committee hereby designates the Business Administrator as the LCCTC Privacy Officer who will, with individuals appointed by the Administrative Director as members of a "Privacy Team," undertake the necessary tasks to ensure compliance with the HIPAA Privacy Rule.

5. Policy Standards for Privacy and Security

General Standards

1. In order to protect the individually identifiable health information entrusted to the Plans, no "protected health information" shall be disclosed by the Plans except as permitted or required by Sections 164.502(a), 164.502(b), and Section 164.504(f) of the Privacy Rule, and as otherwise permitted by the Privacy Rule.

2. All individually identifiable health information of the Plans in any medium shall be maintained in a central depository for the Plans under the control of the Privacy Officer.

3. Only LCCTC employees involved in the administration functions of the Plans shall have access to protected health information.

4. Those LCCTC employees with access to individually identifiable health information of the Plans shall be restricted to the minimum number reasonably necessary to perform administrative functions of the Plans. Persons with access to protected health information of the Plans may only have such access on a need to know basis and must be approved as an "authorized data user" prior to access thereto by the Privacy Officer.

5. It is the responsibility of every authorized data user to maintain confidentiality of individually identifiable health information of the Plans even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.

6. Individually identifiable health information is the property of the individual to whom the information pertains and the Plans are the steward of that information and the owner of the storage medium.

7. Protected health information of the Plans may not be disclosed for purposes of employment related actions, nor for any other purpose prohibited by the Privacy Rule (see, for example, Section 164.504(f)(3)).

Personnel Designations

1. The Privacy Officer is responsible for the coordination and implementation of this Policy; the development from time to time of any appropriate amendments or additions to the Policy and its procedures; cataloging individually identifiable health information of the Plans; receiving complaints; assisting the beneficiaries of the Plans on the interpretation of this Policy; preparing and providing information regarding the Plans' Notice of Privacy Practices; monitoring and tracking violations and appeals; identifying areas of risk with the Information Security Officer; defining with the Information Security Officer security controls; training and education; and supervising maintenance of records of authorized users. The Privacy Officer shall have additional duties as are from time to time delegated by the LCCTC administration in furtherance of matters related to this Policy. The Privacy Officer will also serve as the Information Security Officer. The Privacy Officer may also delegate specific duties to a specific person designated as the HIPAA Contact Person. The Contact Person will be responsible for:
    a. Receiving complaints concerning the Privacy Policies and Procedures,
    b. Receiving complaints concerning compliance with the Privacy Policies and Procedures or with the requirements of the Privacy Rule generally, and
    c. Providing further information about matters covered by the Notice of Privacy Practices.

2. The Information Security Officer (or "Security Officer") is responsible for the design, development and implementation of security procedures and requirements for the gathering, storing, transmission and security of the Plans' information and data processing and computer information technologies, and for its compliance with the standards adopted pursuant to HIPAA and other law and applicable to the Plans from time to time. Without limiting the generality of the foregoing, the Information Security Officer is responsible for determining appropriate security measures and creating procedures that monitor and control access to system resources and data of the Plans. This Information Security Officer will update security standards as necessary and is responsible for the prevention, detection, containment and correction of security breaches.

Complaints; Correction of Data

1. The Privacy Officer is responsible for all complaints. Individuals have the right to correct inaccurate individually identifiable health information under the Plans' control. The appropriate process for validating and processing such corrections is determined individually by the Privacy Officer.

2. The Privacy Officer is responsible for ensuring that validated correction requests relevant to individually identifiable health information of the Plans is implemented.

3. To the extent that an audit trail shows access to a Plan beneficiary's individually identifiable health information, it shall be made accessible to that individual at the individual's request in the event that questions arise about improper access to his or her records.

4. The Privacy Officer shall document all complaints received and their disposition.

Safeguards and Security

1. The Plans, under the direction and authority of the Privacy Officer, shall create, administer and oversee procedures to ensure the prevention, detection, containment, and correction of breaches of security, integrity, and confidentiality.

2. The Plans' security management process shall be the responsibility of the Security Officer, under the general supervision of the Privacy Officer, and must include, at a minimum, the implementation of:
    a. Risk analysis;
    b. Risk management, including procedures for monitoring, detection, auditing, reporting, and responding to breaches of security, integrity, and confidentiality;
    c. A disciplinary process including procedures for the potential discipline, up to and including dismissal, for misuse, misappropriation of data, or acts of omission or commission which result in breaches of security, integrity, or confidentiality of protected health information of the Plans.

3. The prevention of access to protected health information of the Plans by unauthorized or untrained personnel shall be addressed by personnel security procedures, including provisions that ensure that all personnel with access or potential access to protected health information of the Plans are specifically authorized for that access, are trained in relevant confidentiality policies, and have attested knowledge of and compliance with those policies.

4. The security management process shall be the responsibility of the Security Officer according to the guidelines set by the Privacy Officer in consultation with the Security Officer and such other individuals and consultants as the Privacy Officer deems appropriate, and must include, at a minimum procedures to limit physical access while ensuring that properly authorized access is allowed.

5. Certain individually identifiable health information, such as information regarding HIV, substance abuse, sexual abuse, mental health, and psychotherapy notes, are subject to additional specific legal restrictions. Disclosure to anyone other than the individual in question or for treatment, payment or health care operations of such information shall only be made as permitted by this Policy and appropriate law.

Training

1. All applicable employees performing functions for the Plans shall receive education and training on the expectations, knowledge, and skills related to information security and the requirements of this Policy and the Privacy Rule prior to April 14, 2004, and upon any material change in this Policy or the Privacy Rule, and in addition, as to new employees performing functions for the Plans, prior to being given access to protected health information of the Plans. The Privacy Officer shall verify and document the training and that employees performing functions for the Plans have received required education and training and attested to this Policy on an annual basis

2. The employees performing functions for the Plans shall receive training with respect to any material change to the Policy within a reasonable time after its implementation.

Sanctions and Mitigation

1. Should evidence of data access or disclosure of protected health information outside that granted and permitted under this Policy be discovered, it may result in disciplinary action, up to and including termination of employment.

2. Failure to follow the requirements of this Policy are subject to appropriate disciplinary action up to and including termination of employment.

3. All sanctions will be documented in accordance with LCCTC employee policy.

4. The Plans shall mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information in violation of this Policy.

Notice of Privacy Practices

1. The Plans' Notice of Privacy Practices is attached to this Policy and is incorporated into this Policy.

2. The Privacy Officer is responsible for maintenance of the Notice of Privacy Practices.
    a. The Notice of Privacy Practices shall be distributed to all Plan beneficiaries on or before April 14, 2004; thereafter to each new enrollee at the time of enrollment; and to individuals covered by the Plans, within sixty (60) days of a material revision to the Notice.
    b. Not less frequently than once every three (3) years, the Plans will notify Plan beneficiaries of the availability of the Notice and how to obtain the Notice.