Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Administrative Simplification Statute and rules mandate federal protection for individually identifiable health information. The Privacy Rule set out the national standards for health information created by three types of covered entities: health plans, health-care clearinghouses and health care providers.

The university is committed to compliance with all requirements of HIPAA and its implementing regulations as they may be amended.

University Rule 3361:10-5-20 passed by the Board of Trustees in June 2011, designated the university as a hybrid entity. A hybrid entity is an organization that has components covered by the Privacy Rule.

This policy addresses appropriate guidelines and procedures for university compliance with HIPAA regulations.

Components

The following are designated health care components subject to the HIPAA requirements:

1. University Health Services;
2. Hoxworth Blood Center;
3. College of Medicine;
4. College of Nursing;
5. Winkle College of Pharmacy;
6. College of Allied Health Sciences;
7. College of Education, Criminal Justice and Human Services;
8. Joint Center for Health Informatics;
9. Human Resources/ university health benefits plans;
10. Office of Vice President for Legal Affairs and General Counsel;
11. UC Information Technologies (UCIT) Office of Information Security (OIS);
12. Office of Research compliance & regulatory affairs;
13. Internal Audit; and
14. Such other components as may be required to comply with the changes in the law or that are necessary for the orderly operation of the university as determined in writing by the vice president for legal affairs and general counsel in consultation with the senior vice president for academic affairs and provost.

These departments may use protected health information (PHI) for uses and disclosures that are permitted by the Privacy Rule.

Definitions

Definitions of key terms used in this policy can be found in Appendix A.

Policy

Below are entity policy statements for the following:

- Designated Privacy Official
- Retention of HIPAA Related Documents
- Workforce HIPAA Training
- No Retaliation
- Reasonable Safeguards
- Mobile Devices
- Business Associates
- Sanctions

Designated Privacy Official
UC must designate a Privacy Official to serve as a contact person for HIPAA. Overall administration of the university's HIPAA compliance program shall be the responsibility of the privacy official who is appointed by and reports to the vice president for legal affairs and general counsel.

Retention of HIPAA Related Documents
HIPAA requires that all documents be retained for six years from the date of creation or the date it was last in effect. This includes the following documentation:

- Business Associate Agreements
- Acknowledgement of Notice of Privacy Practices
- Authorization Forms
Workforce HIPAA Training
Each member of UC workforce in a covered component must be trained on HIPAA policies and procedures as necessary for their job function within a reasonable amount of time after the individual joins UC. Each covered component will assure that training is completed as soon as possible but no later than 60 days after employment begins.

1. Changes in Policies and Procedures: When there is a material change to the HIPAA regulations, UC policies and procedures may be revised to comply with the new provisions. Each workforce member affected by the change will be trained on the new policies and procedures within a reasonable amount of time.

2. Documentation: UC must document or track that training has been provided and maintain the documentation in written or electronic form for six years from the date of its creation.

No Retaliation
UC may not retaliate against any individual for the exercise of any right under the Privacy Rule including filing a complaint with the Secretary, Department of Health and Human Services or Office for Civil Rights.

Reasonable Safeguards
UC is required to use reasonable administrative, technical and physical safeguards to protect Protected Health Information (PHI) from any intentional or unintentional uses and disclosures in accordance with the HIPAA regulations.

Procedures for reasonable safeguards of PHI can be found in Appendix B, which includes information on PHI storage, PHI disposal, email and other safeguards.

Mobile Devices
Mobile devices that are used to receive transmit or store PHI must be secured.

Procedures for securing mobile devices can be found in Appendix B.

Business Associates
The federal HIPAA regulations on patient privacy and confidentiality limit how PHI can be used by and disclosed to outside persons and entities that provide health care operation services for UC. UC may disclose PHI to a business associate (BA) and may
allow it to create, receive or use PHI on its behalf if UC receives reasonable assurances that the BA will safeguard the PHI. The assurances must be in the form of a written Business Associate Agreement which contains the required elements described in the Privacy Rule.

**Sanctions**
UC must apply sanctions against members of its workforce who fail to comply with its privacy policies and procedures or the requirements of the Privacy Rule.

Procedures for sanctions can be found in [Appendix B](#).

**Uses and Disclosures**

Below are Uses and Disclosures policy statements for the following:

- Uses and Disclosures of PHI
- Disclosures to Law Enforcement
- Authorization for Use and Disclosure
- Minimum Necessary
- Notice of Privacy Practices
- Acknowledgement of Receipt of Notice of Privacy Practices
- Use and Disclosure of Protected Health Information for Research
- Use and Disclosure of Protected Health Information for Fundraising
- Use and Disclosure of Protected Health Information for Marketing
- Benefits Plan Use and Disclosure of Protected Health Information
- Disclosures to Family and Friends

Procedures for uses and disclosures of PHI can be found in [Appendix C](#).

**Uses and Disclosures of PHI**
The federal HIPAA regulations on patient privacy and confidentiality permit disclosure of PHI for treatment, payment and health care operations without patient authorization. All other disclosures must be with authorization unless they meet another exception or are required by law.

1. UC may use and disclose PHI for the following purposes:
   A. For its own treatment, payment and health care operations;
   B. To a health care provider for treatment;
   C. For the payment activities of another covered entity or health care provider;
   D. For the health care operations of another covered entity or health care provider if each entity has or has had a relationship with the individual who is the subject of the PHI requested and the disclosure is for one of the defined health care operations purposes or for detection of health care fraud and abuse;
E. To another covered entity that participates in an organized health care arrangement with UC for any health care operation activities of the organized health care arrangement;
F. To arrange for an organ transplant;
G. For research purposes with institutional review board (IRB) approval and IRB waiver of authorization if required;
H. To the armed forces for members of the military as required; and
I. To worker’s compensation agencies.

2. Uses and disclosures of PHI for purposes other than treatment require that only the minimum necessary amount of information be used for the used or disclosure. See Minimum Necessary policy statement.
   A. In order for UC to use and disclose PHI for purposes other than those listed above, see other UC HIPAA policy statements that describe how Disclosures to Law Enforcement, Disclosures to Friends and Family involved in the care of the patient, Use and Disclosure for Marketing, and Use and Disclosure for Fundraising may be made.

3. Psychotherapy Notes may not to be disclosed unless UC obtains a signed authorization by the patient or legal representative prior to disclosure.

4. UC may disclose PHI for notification purposes:
   A. To notify or assist in the notification (including identifying or locating) a family member, personal representative, or another person responsible for the care of the individual, of the individuals location, general condition, or death.
   B. To assist an entity authorized by law to assist in disaster relief efforts, for the purpose of coordinating relief efforts, assistance in notification, or notification of a family member, personal representative, or another person responsible for the care of the individual, of the individuals location, general condition, or death.

5. UC is required to disclose PHI if it is mandated by state or federal law.

Disclosures to Law Enforcement
The federal HIPAA regulations on privacy, security and confidentiality specify that PHI may be disclosed to a law enforcement official under specific circumstances. Unless required by law, disclosure to law enforcement is permitted by HIPAA but disclosure is not mandatory.

Authorization for Use and Disclosure
The federal HIPAA regulations on privacy and confidentiality restrict the ability of UC to use and disclose individual PHI in many circumstances. PHI may be used by the covered entity for treatment, payment or other health care operations purposes. For other uses and disclosures when the authorized requestor makes a request or when they authorize UC to use their PHI for purposes other than treatment, payment or health
care operations, the requestor will be required to complete the Authorization for Release of PHI form (see Related Links).

**Minimum Necessary**
The federal HIPAA regulations on privacy and confidentiality require in many cases that only the minimum necessary PHI may be used, requested or disclosed. It is the policy of UC to limit uses, disclosures, and requests for PHI to that which is reasonably necessary to accomplish the intended purpose of the use, disclosure or request for payment and health care operations purposes and other non-treatment functions.

**Notice of Privacy Practices**
The federal HIPAA regulations on patient privacy and confidentiality require that a Notice of Privacy Practices be distributed to every patient or their legal representative and made available to the public which describes how PHI may be used and disclosed by UC.

**Acknowledgement of Receipt of Notice of Privacy Practices**
An Acknowledgement of Receipt of Notice of Privacy Practices must be obtained from each individual or their legal representative at the time they receive a copy of the Notice of Privacy Practices.

**Use and Disclosure of Protected Health Information for Research**
The federal rules on privacy and confidentiality (HIPAA) allow UC to use and disclose PHI for research purposes with documentation of patient authorization, research study informed consent combined with patient authorization, or a waiver of authorization issued by an Institutional Review Board (IRB) or Privacy Board.

**Limited Data Set**
The federal rules on privacy and confidentiality (HIPAA) allow UC to use or disclose a Limited Data Set (LDS) of PHI under certain circumstances when a Data Set Agreement (DSA) is entered into between UC and the researcher. UC may use or disclose a LDS set for research, public health studies or for the health care operations of another covered entity without authorization when UC has received satisfactory assurances from the recipient in the form of a DSA that the recipient will only use or disclose the PHI for limited purposes.

**Use and Disclosure of Protected Health Information for Fundraising**
The federal HIPAA regulations on privacy and confidentiality limit how protected health information may be used and disclosed for fundraising activities.

**Use and Disclosure of Protected Health Information for Marketing**
The University of Cincinnati (UC) collects and maintains patient protected health information (PHI). The federal HIPAA regulations on patient privacy and confidentiality prevent a covered entity from using or disclosing protected health information (PHI) for marketing purposes without a signed authorization.
Benefits Plan Use and Disclosure of Protected Health Information
UC offers various health plans to its employees and retirees. UC’s self-funded plans, Flexible Spending Accounts and Health Savings Accounts are components subject to the HIPAA requirements. UC Benefits Plan must maintain the privacy of PHI.

Disclosures to Family and Friends
The federal HIPAA regulations on individual privacy and confidentiality allow UC to disclose PHI to friends and family that are involved in the care of the patient. At times UC may find it necessary, or in the best interest of an individual’s care to disclose certain relevant PHI to family members or friends who may be involved in the care or payment related to the individuals care.

Individual Rights under HIPAA

Below are policy statements for individual rights under HIPAA as follows:

- Request for Restriction of Protected Health Information
- Confidential Communications
- Access to Protected Health Information
- Amendment of Protected Health Information
- Accounting of Disclosures of Protected Health Information
- Notification of Breach of Unsecured Protected Health Information
- Privacy Complaints

Procedures for individual rights under HIPAA of PHI can be found in Appendix D.

Request for Restriction of Protected Health Information
The federal HIPAA regulations on privacy and confidentiality allow individuals the right to request certain restrictions on the uses and disclosures of PHI that UC may make. UC is not required to agree to a restriction.

Confidential Communications
The federal HIPAA regulations on individual privacy and confidentiality allow individuals the right to request that communications from UC be made by an alternative means or at an alternate location. UC must accommodate reasonable requests for confidential communications.

Access to Protected Health Information
The federal HIPAA regulations on individual privacy and confidentiality allow an authorized requestor the right to access certain PHI contained in their records.

Amendment of Protected Health Information
The federal HIPAA regulations on individual privacy and confidentiality grant individuals the right to request an amendment to PHI in their medical record. UC is not required to grant the request.
Accounting of Disclosures of Protected Health Information
UC is required and/or permitted to disclose that information to many of its business associates and other entities for a variety of reasons. The federal HIPAA regulations on individual privacy and confidentiality grant authorized requestors the right to receive an accounting of many of the disclosures that are not for the purpose of treatment, payment or health care operations that it has made of their PHI.

Notification of Breach of Unsecured Protected Health Information
The federal Health Information Technology for Economic and Clinical Health Act (HITECH) regulations on privacy and security of PHI require notification to the individual whose unsecured PHI has been or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as a result of the breach.

See the HIPAA Definitions in Appendix A for definitions of Breach and Unsecured PHI, and to the Secretary, Office for Civil Rights (OCR) and mitigation of harm in the event of the breach of unsecured PHI.

Privacy Complaints
The federal HIPAA regulations on patient privacy and confidentiality require UC to establish a process for individuals to make a complaint concerning its privacy policies and procedures or compliance with the policies and procedures.

Related Links:
Each form should be listed here in alphabetical order
- Appendix A – Definitions
- Appendix B – Reasonable Safeguards for PHI Procedures
- Appendix C – Uses and Disclosures of PHI Procedures
- Appendix D – Access and Communications Procedures
Information Security and HIPAA

Phone Contacts:
Director of Privacy 556- 3483
Information Security 558- 4732