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 or are units that perform activities in support of these components which would qualify as business associates if they were separate legal entities and are therefore subject to the HIPAA requirements:
1. University Health Services: Records of patients who are not students of the University are designated and maintained in accordance with HIPAA. Records of patients who are students of the University are designated and maintained in accordance with FERPA.
2. Hoxworth Blood Center;
3. College of Medicine;
4. Joint Center for Health Informatics;
5. Human Resources/university health benefits plans;
6. Office of Vice President for Legal Affairs and General Counsel;
7. UC Information Technologies (UCIT) Office of Information Security (OIS);
8. Office of Research Integrity;
9. Internal Audit; and
10. 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.

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 shall 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
Request for Restriction
Request for Access
Request for Amendment
Request for Accounting of Disclosures
Training
Privacy Complaints
Versions of the HIPAA Policies and Procedures
Any action, activity or designation required by the Privacy Rule

**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. UC faculty who are workforce members of affiliated covered entities (UC Health, Cincinnati Children’s Hospital Medical Center, Veterans Affairs Medical Center) may satisfy the training requirement through the affiliated covered entity’s required training. UC will verify that training has been completed in accordance with the covered entity’s requirements.

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.

3. **Failure to complete training:** Training is mandatory. Failure to comply with training requirements will result in disciplinary action in accordance with collective bargaining agreements and human resource policy.

**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; 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;
E. To arrange for an organ transplant;
F. For research purposes with institutional review board (IRB) approval and IRB waiver of authorization if required;
G. To the armed forces for members of the military as required; and
H. 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 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 healthcare 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
HIPAA allows 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
HIPAA allows 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. UC may terminate Recipient’s use of the Limited Data Set at any time that UC has reason to believe that Recipient has violated any of the conditions of the Agreement or has accessed any information for any purpose not described in the Agreement.

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 asserting individual rights to PHI under HIPAA 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:**

Privacy Official 556-3483
Information Security 556-0803
Access - The ability to inspect, review or receive a copy of protected health information (PHI) held in a designated record set.

Authorization - A permission to use and disclose specific PHI identified for limited purposes requested. Authorizations must have a limited duration and may only be relied upon for that period of time.

Authorized Requestor - An individual who is the subject of the PHI or their legal representative, who is authorized to make health care decisions on behalf of the individual. For example, a court appointed legal guardian, a parent or guardian of a minor child, a health care power of attorney or a general power of attorney.

Benefits plan – An individual or group plan that provides or pays the cost of medical care.

Breach - The acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Business Associate - A person or organization that performs a health care operation function or activity on behalf of UC that is not part of UC’s workforce that involves the use or disclosure of PHI. A business associate may be a covered entity in its own right. The business associate must provide satisfactory assurances that it will appropriately safeguard PHI that it uses or discloses on behalf of its work for UC.

Business Associate Agreement - A written document that lists the business associates obligations and responsibilities and agreement to protect the PHI that it uses or discloses on behalf of the hybrid entity.

Confidential Communication - A private communication made to an individual at an alternative location or by alternative means.

Covered Component - A university department or area that performs functions that make it a health plan or health care provider subject to the Privacy Rule.

Covered Entity - A health plan or health care provider that transmits any health information in an electronic form in conjunction with a transaction covered by HIPAA. For example, PHI that is held in paper or electronic format that is billed for electronically.

De-identified Protected Health Information - Health information that does not identify an individual, and where there is no reasonable basis to believe that the information can
be used to identify the individual. Removal of identifiers with a method described by the Secretary, Department Health and Human Services will render PHI de-identified.

The Safe Harbor de-identification method requires the removal of 18 types of identifiers of the individual or of relatives, employers or household members of the individual:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   A. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   B. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographs and any comparable images
18. Any other unique identifying number, characteristic, or code; and

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

**Designated record set** - A group of records maintained by or for the covered entity that is the medical records and billing records about individuals maintained by or for a health care provider; the payment, claims adjudication, and case or medical management record systems maintained by or for health plan; or used in whole or in part, by or for the covered entity to make decisions about individuals.
**Disclosure** - The release or divulgence of protected health information whether verbal, electronic or on paper to a person, institution or entity that is not a part of UC.

**Electronic Protected Heath Information (ePHI)** is individually identifiable health information transmitted by electronic media or maintained in electronic media.

**Encryption** - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and that process or key and such confidential process or key that would allow decryption has not been breached. The US Department of Health and Human Services (HHS) has identified certain encryption processes that meet this standard, including encryption processes for data at rest that are consistent with National Institute of Standards and Technology (NIST) standards.

**Health care component** – A component or combination of components of a hybrid entity designated by the hybrid entity.

**Health Care Operations** - Any of the following activities of the hybrid entity to the extent the activities are related to functions covered by HIPAA: quality assessment and improvement, development of clinical guidelines, case management and care coordination, contacting patients with information about treatment alternatives, reviewing the qualifications of health care professionals, conducting training programs in which students, trainees or practitioners in areas of health care learn under the supervision to practice or improve their skills as health care providers, certification, licensing or credentialing activities, conducting medial review, legal services, and audit functions, business planning, business management, compliance, customer services, data analysis and risk management.

**Health care provider** - A provider of medical or health services and any other person or organization who furnishes, bills or is paid for health care in the normal course of business.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)** - Standards for Privacy of Individually Identifiable Health Information; Final Rule 45 CFR Parts 160 and 164. This federal rule includes standards to protect the privacy of individually identifiable health information and became effective April 14, 2003.

**The Health Information Technology for Economic and Clinical Health Act (HITECH)** - A federal act that promotes health care technology. It amends the HIPAA privacy rule and requires breach notification in the event of a breach of unsecured PHI. HITECH increases enforcement of HIPAA and increases the fines and penalties for violations.

**Hybrid entities** - Covered entities with different components that perform health care and non-health care activities and whose covered health care functions are not their primary functions, such as universities.
Incidental use or disclosure - A secondary use or disclosure that cannot be reasonably prevented, is limited in nature and occurs as a byproduct of an otherwise permitted use or disclosure.

Individual - The person identified as the subject of the PHI created by UC.

Individually identifiable health information - A subset of protected health information that includes demographic information collected from an individual and is created or received by a hybrid entity. This information relates to the past, present or future physical or mental health or condition of an individual.

Institutional Review Board (IRB) - A specially constituted review body established by an entity to protect the welfare of human subjects recruited to participate in clinical research. Under HIPAA the IRB can review and approve waivers of authorization to use and disclose PHI for research purposes.

Licensed Health Care Professional - A provider of medical or health care services with a license provided by state entity with licensing authority.

Limited Data Set (LDS) - PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. postal address information, other than town or city, state and ZIP code;
3. telephone numbers;
4. fax numbers;
5. Email addresses;
6. Social Security numbers;
7. medical record numbers;
8. health plan beneficiary numbers;
9. account numbers;
10. certificate/license numbers;
11. vehicle identifiers and serial numbers, including license plate numbers;
12. device indicators and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. biometric identifiers; including finger and voice prints; and
16. full face photographic images and any comparable images.

A LDS may include city, state, ZIP code and age. Birth date may be included if researcher and entity agree that it is necessary for the purpose of the research.

Minimum Necessary - Minimum necessary is the least amount of PHI that is used to accomplish the intended purpose of the use, disclosure, or request. Minimum necessary does not apply to disclosures to or requests by a health care provider for treatment;
uses or disclosure made to the individual, as permitted by authorization, for uses and
disclosures as required by law and for uses and disclosures used for compliance with
HIPAA.

**Mobile device** – A handheld transmitting device with the capability to access, transmit,
receive, and store PHI. Examples of mobile devices include smartphones, tablets, and
laptops.

**Notice of Privacy Practices** - A written document that is given to individuals that
addresses how the individuals’ health care information will be used and disclosed and
an individual’s rights over their PHI.

**Office for Civil Rights (OCR)** - The division of the Department of Health and Human
Services responsible for enforcement of the HIPAA privacy and security rule.

**Payment** - The activities undertaken by the health care provider or health plan to obtain
or provide reimbursement for the provision of health care.

**Privacy complaint** – A complaint filed when there is a belief that a component of the
hybrid entity or its business associate violated an individual’s privacy rights or
committed another violation of the Privacy, Security or Breach Notification Rules.

**Privacy Officer** - An official designated by UC to develop and implement privacy
related policies and procedures.

**Personal Representative** – a person who has the legal authority to act on behalf of an
individual in making health care decisions.

**Protected Health Information (PHI)** - Individually identifiable health information that is
transmitted electronically, maintained in any electronic medium, or transmitted or
maintained in any other form or medium. This information has been created or received
by a health care provider, health plan, public health authority, employer, life insurer,
school or university or health care clearinghouse that relates to the past, present and
future physical and mental health, provision of health care to the patient and payment
for the patient’s health care.

**Psychotherapy notes** - Notes that are recorded, either orally, in writing or electronically
by a mental health professional who is documenting or analyzing a conversations during
a counseling session whether it is with one individual or a group. The notes do not
include medication prescription and monitoring; the forma and frequency of treatment,
clinical test results; or summaries of diagnosis, functional status, there treatment plan,
symptoms, prognosis and progress. The notes are separated from the rest of an
individual’s medical record.

**Required by Law** - A mandate contained in law that compels a covered 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 or a governmental or administrative body and a civil or an authorized investigative demand.

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

**Treatment** - 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 providers relative to a patient; or the referral of a patient for health care from one health care provider to another.

**Unsecured Protected Health Information** - PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

**Use** - The release of information within the covered entity for utilization to carry out treatment, payment or health care operations.

**User** - A person or entity with authorized access to specific PHI.

**Workforce** - Employees, volunteers, trainees and other persons under the direct control of a covered entity, regardless of whether or not they are paid by the covered entity.
This Appendix covers procedures for reasonable safeguards of PHI, which includes information on PHI storage, PHI disposal, email and other safeguards.

**Reasonable Safeguards Procedures**

The HIPAA regulations permit incidental uses and disclosures of PHI that occur as a by-product of another permissible use or disclosure as long as reasonable safeguards are applied. All UC employees are expected to use professional judgment based on their job on a case by case basis to determine what reasonable safeguards to apply.

1. **PHI Storage**

   A. Patient charts, records, reports, images, and other documents or media containing PHI must be stored securely. The means for securing such information must be appropriate to the location and risk of unauthorized access. For example, files and charts containing PHI must not be accessible in public areas and should be locked when not in use.

   B. Paper records that are placed outside a patient’s room in clinical areas should be placed with the name facing the wall.

   C. In secure areas, PHI should be put away or locked in the desk or office when not in use. In non-secure areas patient records that are in use with an employee present should be turned face down when not in direct use and filed or disposed of properly when no longer needed.

2. **PHI Disposal**

   A. Secure methods must be used for disposal of PHI. This applies to all types of PHI including paper, electronic and other forms such as plastic, labels and other materials containing or printed with PHI.

   B. Paper PHI should not be disposed of in the regular trash, recycling bin or hazardous waste bin.

   C. Secure methods for disposing of PHI including shredding of paper PHI or disposal in a locked shred bin provided by a reputable vendor.

   D. If accessible to the public, shred bins must be locked and secured to prevent access.

   E. For disposal of media containing electronic PHI refer to the guidelines of the information security department.
F. Displays of PHI / Computer Screens Computer screens should be positioned so that PHI is not easily viewed by unauthorized persons.

G. Log out of computer when finished using PHI. Computers should not be left unattended when logged in to patient records.

H. Log-in information or passwords should never be shared with anyone else.

3. Conversations

A. Staff should not discuss PHI in elevators, hallways, where other individuals are present and in public areas.

B. When circumstances permit, speaking should be in private.

C. Private areas should be used to discuss patient condition with patients’ family and friends.

D. For discussion of PHI with a patient when there is another person present with the patient informs the patient the discussion may disclose PHI and either:
   i. The patient should be asked if they would like the person present during the conversation; or
   ii. The person present with the patient should be asked to leave the room during your discussion with the patient.

4. PHI transfer from location to location

A. PHI carried from location to location between facilities must be secured during transfer. Employees who physically deliver records are responsible to ensure that the PHI is left at the destination in a secure manner. During transfer the PHI should be in a sealed envelope marked “Confidential” and should clearly indicate the name and location of the intended recipient and sender.

B. PHI that is taken out of the institution must be secured and locked up on transfer, for example in the trunk of the car.

C. PHI that is transferred between locations should contain contact information within on what to do if the information is lost or misplaced and someone finds the PHI.

5. Printers

A. Printers should be located in a low traffic area that is not accessible to those not authorized to receive the information.

6. Fax Machines

A. A UC fax cover sheet must be used with all faxes sent that contain PHI. The cover sheet must contain a confidentiality statement and contact information for the recipient in the event the fax is received in error.
B. Fax machines should be located in a low traffic area that is not accessible to those not authorized to receive the information.
C. The fax number of the recipient should be confirmed prior to sending a fax by calling the person or office to which the fax will be sent.
D. When faxes are regularly sent to the same recipients or the numbers are programmed into the machine’s memory, the numbers should be checked regularly to verify that the number is still in operation.

7. Sign in lists

A. A sign in list is permitted as long as there is no PHI displayed on the sheet.
B. Information on the sign in sheet must not include any information that includes diagnosis or condition.

8. Email

A. Emails sent to the following partner sites are automatically secured: UCHHealth.com, UCPhysicians.com, and CCHMC.com (Cincinnati Children’s Hospital Medical Center).
B. To ensure that emails to other sites over the internet are sent in a secure manner, type the work encrypt as the first word in the subject line.
C. Place a confidentiality statement on the email and contact information for the recipient in the event an email containing PHI is received in error.

9. Voice Mail and Answering Machines

A. It is permissible to leave a message with a family member or other person that answers the patient’s telephone, on an answering machine or on a voice mail when the patient does not answer the telephone.
B. The information should be limited to the minimum necessary amount of information.

10. Laptop and Personal Computers

A. Laptop and personal computers must have an encrypted hard drive if PHI is saved to it.
B. PHI may only be saved to a flash drive or thumb drive that is encrypted.

11. Mobile devices
The reasonable safeguards for protection and security of mobile devices include the following:

A. A password or other user authentication should be used.
B. Encryption should be installed and enabled to protect PHI stored or sent by mobile devices.
C. Remote wiping and/or remote disabling should be installed and activated to erase data on your mobile device if it is lost or stolen.
D. File sharing applications should not be installed or must be disabled.
E. A firewall should be installed and enabled to block unauthorized access.
F. Security software should be installed and enabled to protect against malicious applications, viruses, spyware and malware-based attacks.
G. Security software should be kept up to date.
H. Mobile applications should be researched before downloading.
I. Physical control of your mobile device should be maintained. User should know where it is at all times to limit the risk of unauthorized use.
J. Users should ensure adequate security to send or receive PHI over public Wi-Fi networks.
K. Users should delete all stored PHI before discarding or reusing the mobile device.

Business Associate Agreements
A business associate agreement must identify the uses and disclosures of PHI the business associate is permitted to make and requires the business associate to implement safeguards to protect against a use or disclosure of PHI not permitted by the agreement. UC must take certain actions if a business associate materially violates the Business Associate Agreement.

1. Business Associate Identification: Prior to entering into an agreement or contract with an outside entity who will perform a service for or on behalf of University of Cincinnati that will receive or use PHI in order to perform this activity or service, determine if a business associate agreement is required.
   A. Some examples of business associates are: data analysis or aggregation companies, third-party billing companies, collection agencies, outside legal services, actuarial services, accounting services, consulting services, nursing and other professional temporary staffing agencies, temporary office staffing and accreditation services. An example of who is not a business associate is an outside service that is not given PHI in order to perform services for UC. If unsure whether an individual or entity is a business associate, contact the UC Privacy Officer or Office of General Counsel for guidance.
   B. If a Business Associate Agreement is required, use the standard UC Business Associate Agreement form.

2. Signed Agreement Required: The Business Associate Agreement must be in writing and contain the signature of the business associate.

3. Notice of Breach: On receipt of information that business associate has violated the business associate agreement, the employee receiving the information must notify UC Privacy Officer. The Privacy Officer will investigate the alleged violation and take the necessary actions to cure the breach or end the violation. If the
business associate agreement was materially breached, actions may include termination of the underlying contract. If termination is not feasible, the Privacy Officer may report the violation to the Department of Health and Human Services, Office for Civil Rights.

Sanctions

A. Failure to comply with the Health Insurance Portability and Accountability Policy may result in disciplinary action in accordance with collective bargaining agreements and human resource policy.
This Appendix covers procedures related to Uses and Disclosures of PHI.

**Disclosures to Law Enforcement**

The reason for the request needs to be determined: The ability to disclose PHI to a law enforcement agent depends on the circumstances of the situation and the reason for the request. It is important to determine the reason for the request as well as the type of PHI the agent is requesting.

1. **Required by law:** HIPAA permits disclosure of PHI without authorization of the individual when federal or state law requires it. If required by law, the person receiving the request should inquire under what law the officer is requesting the disclosure. The identity of the officer should be verified as well as the law he/she is citing before making the disclosure.

2. **Disclosure should be limited to the minimum necessary:** If disclosure is made it must be limited to the extent necessary to satisfy the request. Only information that is specifically requested may be disclosed.

3. **Subject to search warrant, court order or grand-jury subpoena:** PHI may be released to a law enforcement agent if the agent presents a court order, search warrant or in some circumstances a grand-jury subpoena. Disclosure must be limited to that specifically requested in the document. The Privacy Officer and UC General Counsel’s office should be notified immediately if a warrant, court order or grand-jury subpoena for PHI is received.

4. **Subject to a subpoena:** If an agent presents a subpoena that is signed by the Clerk of Court the Privacy Officer and UC General Counsel's should be notified office immediately.

5. **Subpoena, summons, or investigative demand from an administrative court or tribunal.** The Privacy Officer and UC General Counsel's office should be notified immediately upon receipt of an administrative subpoena, summons or investigative demand either in person or by mail delivery.

6. **Disclosure with individual authorization:** PHI may be released if an officer presents an Authorization for Release of PHI signed by the individual or legal representative with the subpoena.
7. Disclosures when there is suspected child abuse: Disclosure of PHI relating to alleged child abuse, neglect or exploitation is permitted as required by state law. In Ohio physicians and other health care providers are required to report any suspected case of child abuse to law enforcement by Ohio law (O.R.C. § 2921.22).

8. Other disclosures required by law:
   A. Ohio law requires physicians and other health care providers to report to law enforcement any gunshot or stab wound that the provider observed or any other serious physical harm that the provider reasonably believes resulted from a violent offense (O.R.C. § 2921.22). Law enforcement agents may obtain copies of records related to any drug or alcohol test administered to a person to determine the presence of alcohol or drugs in the person’s system at any time relevant to a criminal offense in question (O.R.C. § 2317.022). Officials must use the specific form provided in the Ohio Revised Code to request these test results (O.R.C § 2317.022).

9. Victim of a crime, including abuse, neglect or domestic violence: UC is permitted to disclose PHI in response to a law enforcement official’s request for information about an individual who is suspected to be a victim of a crime. A signed authorization should be obtained unless the individual is unable to agree due to incapacitation or other emergency circumstance, provided that the law enforcement official represents that the information is needed to determine whether a violation of the law has occurred by a person other than the victim and the information will not be used against the victim; the investigation would be adversely affected by waiting for the individual to agree; and the disclosure is in the best interest of the individual as determined by the Privacy Officer and UC General Counsel’s Office. If an authorization is not obtained in advance, the individual or authorized representative should be notified that a report has been made. UC may choose not to notify if UC determines that notifying would place the individual at risk, or that the personal representative is responsible for the alleged crime and informing is not in the best interest of the individual.

10. To alert law enforcement of a death: UC may disclose PHI to law enforcement officials to alert them to a death that UC suspects may have resulted from criminal conduct.

11. To locate or identify a suspect: If a law enforcement agent requests information to locate or identify a suspect or fugitive or material witness or missing person, limited disclosure may occur. This information includes: individual’s name, address, date and place of birth, Social Security number, blood type and Rh factor, type of injury, date and time of treatment, date and time of death (if applicable) and a description of distinguishing characteristics. No disclosure of PHI concerning individual’s genetic information, DNA analysis, dental records, typing or samples or analysis of body fluids or tissue may occur.

12. Disclosure when a crime has been committed on the premises: Disclosure is permitted if the information relates to a crime committed on UC premises. The
information may be released to the law enforcement agent if UC employee believes in good faith that the PHI is evidence of criminal conduct that occurred

13. UC may disclose PHI to a correctional institution or law enforcement official who has lawful custody of an inmate if law enforcement represents that the PHI is necessary for provision of health care to the individual, the health and safety of the individual, other inmates, officers or other persons responsible for the inmate.

14. To prevent serious or imminent harm: PHI may be disclosed to a law enforcement agent if the individual believes in good faith that the disclosure is necessary to prevent or lessen the threat of serious and immediate harm occurring to someone else.

15. To report injury or death: UC must follow the state law which deal with reporting injuries or deaths, as well as to produce any information to law enforcement as required by such laws.

16. Disclosure for national-security activities: In limited circumstances HIPAA permits providers to release PHI to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national-security activities authorized by National Security Act and implementing authority.

17. Disclosure of information regarding alcohol or drug abuse: Disclosure of information related to treatment for drug or alcohol abuse is subject to federal regulation 42 C.F.R. Part 2 and may occur only under certain circumstances. Refer any request for drug or alcohol treatment information to the Privacy Officer for review.

18. Disclosure of minimum necessary information to law enforcement agents over the phone: May be made with proper identification of law enforcement officer in accordance with the Policy on Verification of Identity.

Authorization for Use and Disclosure

1. *The Authorization for Release of PHI form* (see related link) must be used as appropriate:
   A. When an authorized requestor requests PHI be used or disclosed for purposes other than treatment, payment or other health care operations. For example, in the event an individual would like a copy of their medical record for personal or legal purposes or a copy of psychotherapy notes.
   B. The department that maintains the PHI must obtain a signed Authorization for Release of PHI form and maintain it in the individual's record.
   C. When a use or disclosure of an individual's PHI is requested for UC's purposes, for example for marketing or fundraising.
   D. When a use or disclosure of an individual's PHI is for research for a study that requires the informed consent of the individual.
2. The Authorization for Release of PHI may not be combined with any other consent or authorization form with the exception of authorization for research that includes treatment, which may be combined with the informed consent for the research study.
3. UC may not condition the provision of treatment or payment on the provision by
the individual of any authorization except that research related treatment may be
conditioned on authorization for research related uses and disclosure of the PHI.
Treatment may also be conditioned when the treatment is solely for the purpose
of creating PHI for disclosure to a third party on the provision of an authorization.

4. All uses and disclosures made pursuant to a signed authorization must be
consistent with the terms and conditions of the authorization.

5. Verify the identity of the authorized requestor in accordance with the Verification
of Identity Policy when the legal representative signs the Authorization for
Release of PHI.

6. Revocation of Authorization for Release of PHI; the authorized requestor retains
the right to revoke an Authorization for Release of PHI except to the extent that
action has been taken on it. The revocation must be made in writing to the UC
Privacy Officer at the address on the authorization form.

7. Expiration of Authorization for Release of PHI: The authorized requestor must
indicate on the Authorization for Release of PHI form the intended length of time
for use. If no time is specified the authorization will expire 60 days after it is
signed.

Related Documents
Authorization for Release of PHI Form

Minimum Necessary

1. Disclosures and Uses of PHI which are not limited to minimum necessary
There are some uses and disclosures that are not limited to the minimum
necessary requirements. The following types of disclosures are not limited to the
minimum necessary:
   A. Disclosures to or requests to a health care provider for treatment
      purposes;
   B. Uses, requests, or disclosures made pursuant to an authorization signed
      by an authorized requestor, for example a medical records request;
   C. Uses and disclosures to researchers when there has been an Institutional
      Review Board waiver of authorization or when the researcher has signed
      representation that the PHI will be used only for research protocol
      development or is research on decedents;
   D. Disclosures made to the Secretary of the Department of Health and
      Human Services, Office for Civil Rights for compliance and enforcement of
      the privacy regulations; and
   E. Uses to prepare PHI for and disclosures that are required by law, for
      example disclosures made about victims of abuse, neglect or domestic
violence; and a disclosure made to comply with workers’ compensation laws.

2. Disclosures and Uses of PHI that are limited to the minimum necessary. Disclosures and uses of PHI must be limited to the minimum amount that is reasonably necessary to accomplish the purpose of the disclosure or use. This applies to the PHI used and disclosed for UC payment and health care operations. For example, when disclosing PHI to a commercial insurance company for reimbursement on a medical claim only the minimum necessary information may be disclosed. For UC’s internal accounting or risk management functions only the minimum necessary amount of PHI may be utilized.

3. Routine Uses of PHI: Routine or recurring disclosures, disclosures that are made on a regular basis such as to a health plan for payment purposes or to an internal UC department for health care operations should be limited to the minimum necessary.

4. Non-Routine Disclosures of PHI: Non-routine disclosures of PHI must be reviewed by the UC Department HIPAA Coordinator on an individual basis to assure that only the minimum necessary amount of PHI will be disclosed.

**Notice of Privacy Practices**

1. Timing of Provision: The Notice of Privacy Practices (NPP) must be made available, distributed, and posted in accordance with this policy.

2. Availability to the Public: A copy of the NPP must be made available to any person who requests it in each different building or area where patients receive treatment.

3. Distribution to Patients: All patients must be provided a copy of the UC NPP before or at the time of the first treatment encounter. This may occur either by giving the patient a paper copy of the NPP or by electronic delivery. If UC revises its NPP a revised copy must be offered to the patient the next time the patient receives services. It is the responsibility of the staff to give the patient a copy of the NPP. In the event the patient requires emergency treatment the NPP must be provided after stabilization.
   A. Posting the Notice: Copies of the NPP must be posted in each separate location where patients receive treatment. The NPP must be posted in a clear and prominent location where it is reasonable to expect patients to be able to see and read it.
   B. Website Posting: A copy of the most current NPP must be posted prominently on the UC website.
   C. Revisions to the Notice: When the NPP is revised it must be made available upon request on or after the effective date of the revision. The revised NPP must be distributed, promptly posted at the treatment sites,
and posted on the website. All patients arriving for treatment after the effective date of a revised NPP must be offered the new version.

Acknowledgement of Receipt of Notice of Privacy Practices

1. Provision of Copy of Notice at Admission: At the time of the first encounter with the individual, the UC employee that is registering the individual will provide them with a copy of the Notice and obtain the individual’s or their legal representatives acknowledgement of receipt by having the individual or their legal representative sign the appropriate line on the Acknowledgement of Receipt of Notice Privacy Practices (see Related Links).

2. Individual Previously Received Copy of Notice of Privacy Practices: If the individual or their legal representative has previously received a copy of the Notice and there have been no revisions to the Notice, the individual or their legal representative may sign the appropriate line on the Acknowledgement.

3. Individual Refusal to Accept Notice of Privacy Practices: If the individual or his/her legal representative refuses to accept the Notice of Privacy Practices the employee attempting delivery of Notice should request the individual or their legal representative to sign on the appropriate line.

4. When the Individual is Being Treated for an Emergency Medical Condition: If the individual is being treated for an emergency medical condition the Notice must be given to the individual or legal representative as soon as possible after stabilization.

5. Documentation of Reasonable Efforts to Deliver Notice: If the UC employee is unable to deliver the Notice the employee must sign the Acknowledgement and note what reasonable efforts were made to deliver the Notice. This does not remove the obligation to deliver the Notice as soon as possible.

Related Documents
Notice of Privacy Practices
Acknowledgement of Notice of Privacy Practices

Use and Disclosure of Protected Health Information for Research

1. Research Protocol Development: Reviews preparatory to research. UC may use or disclose PHI for researcher review prior to the development of a research protocol without patient authorization or a waiver granted by an IRB if research is conducted in which the researcher will record only de-identified PHI (see de-identified information list in HIPAA Definitions (Appendix A) and the PHI is not removed from the premises of the covered entity. The primary research investigator must provide a statement to UC that use and disclosure of PHI being sought is necessary to prepare a research study or protocol or similar purposes
preparatory to research, no PHI will be removed from the covered entity by the researcher in the course of the review and the PHI for which access is sought is necessary for research purposes. The researcher must fill out *Researcher Representation for Research Protocol Development form*.

2. Research with Patient Authorization: Patient authorization is required before PHI may be used or disclosed for research, unless there has been an IRB waiver of authorization, or unless it meets one of the exceptions of this section. Authorization will be documented on the *Authorization for Uses and Disclosures of PHI* form (see [Related Links](#)). The Authorization Form must specify an expiration date. The statement “the end of the research study” is sufficient. The authorization for research may be combined with the informed consent for research document.

3. Research with Privacy Board or IRB Waiver of Authorization: UC may use or disclose PHI for research purposes without patient authorization with documentation of a waiver of authorization from an IRB. The UC IRB will review the researcher application for the waiver of authorization and determine if it will grant the waiver. UC may disclose the PHI when it has obtained documentation of the following:
   A. The date the alteration or waiver of authorization was approved;
   B. A statement that the IRB has determined that the alteration or waiver of alteration in whole or in part satisfies the three criteria of the rule;
   C. A brief description of the PHI for which use or access has been determined to be necessary by the IRB;
   D. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
   E. The signature of the chair or other designee of the IRB.

4. Research on Decedents: UC may use or disclose PHI of deceased persons for research without the authorization of the legal representative or waiver of authorization by an IRB with a statement from the primary research investigator that the use or disclosure sought is only for research on the PHI of the decedent and the PHI being sought is necessary for research purposes. UC may request that the researcher provide documentation of the death of the individuals about whom PHI is requested. The researcher must fill out *Researcher Representation for Research on Decedent form* (see [Related Links](#)).

5. Accounting for Research Disclosures: Individuals have the right to receive an accounting of certain research disclosures of PHI made by UC. This accounting must include disclosures of PHI that occurred during the six years prior to the request and must include specified information on each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same
person or entity for a single purpose. Certain disclosures are exempt from the accounting requirement: research disclosures made with an authorization; or disclosures of the limited data set to researchers with a Data Set Agreement (see Related Links).

Related Documents
Researcher Representation for Research Protocol Development form
Authorization for Uses and Disclosures of PHI form
Researcher Representation for Research on Decedent form
Data Set Agreement

Limited Data Set

1. Identification of the Use of the Limited Data Set: When asked for information in a LDS, the UC Department compiling and delivering the data must obtain a signed Data Set Agreement (see Related Links) with the individual requesting the data. The UC Department that receives the request must make a determination whether the stated use of the LDS conforms to the uses allowed by HIPAA which are research, health care operations of another covered entity or public health studies. Examples of health care operations uses include providing the information for another covered entity to use for quality improvement and market share data. An example of use for research includes the creation of a research study or protocol and an example for public health purposes is use by a private disease registry or public health agency for studies in the private or public sector.

2. PHI Permitted in Limited Data Set: A LDS is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

   A. Names;
   B. Postal address information, other than town or city, State and ZIP code;
   C. telephone numbers;
   D. fax numbers;
   E. email addresses;
   F. Social Security numbers;
   G. medical record numbers;
   H. health plan beneficiary numbers;
   I. account numbers;
   J. certificate/ license numbers;
   K. vehicle identifiers and serial numbers, including license plate numbers;
   L. device indicators and serial numbers;
   M. Web Universal Resource Locators (URLs);
   N. Internet Protocol (IP) address numbers;
   O. biometric identifiers; including finger and voice prints; and
   P. full face photographic images and any comparable images.
A LDS may include city, state, ZIP code and age. Birth date may be included if researcher and entity agree that it is necessary for the purpose of the research.

3. Responding to DSA Violations: If UC becomes aware of an activity or practice that constitutes a violation of a DSA by the recipient of the information it is required to notify the UC Privacy Officer. If the violation cannot be cured UC will discontinue disclosure of information to the individual or covered entity.

Related Documents
Data Set Agreement

Use and Disclosure of Protected Health Information for Fundraising

1. Uses of PHI: In preparing fundraising materials and mailing lists for UC fundraising it is permitted to use only the following information collected on current or past individuals:
   A. Demographic information about the individual, including name, address and other contact information, age, gender and insurance status.
   B. Dates of service of health care provided to the individual and department of treatment.
   C. General outcome information which includes non-optimal treatment or services

2. It is not permitted to use any PHI about the individual’s illness or treatment.

3. UC may use a business associate to assist with fundraising. The business associate must sign a Business Associate Agreement prior to UC disclosure of patient information. The business associate may only have access to the same information that UC may access as described above.

4. Opt-out Provision: All fundraising material sent to an individual must include information on how to opt-out of receiving future fundraising material by mail, email or telephone. The Notice of Privacy Practices includes information on where to send a written request to opt-out. When an opt-out request is received, future fundraising materials or communications may not be sent to that individual.

5. Other Uses and Disclosures for Fundraising: Any other uses and disclosures for fundraising on behalf of UC or a third party not described in this policy must be expressly authorized by the individual whose PHI is used or disclosed. The Authorization for Uses and Disclosures of PHI form (see Related Links) must be utilized.

Related Documents
Business Associate Agreement
Authorization for Uses and Disclosures of PHI form
Use and Disclosure of Protected Health Information for Marketing

1. Marketing Authorization Required
   A. Communication about a non-UC facility’s services that is not for the purpose of promoting treatment: A signed Authorization for Release of PHI form (see Related Links) must be obtained before communications are sent to a patient or individual that is for the purpose of promoting a non-UC product or service that is not for treatment.
   B. Disclosures to third parties: A signed Authorization for the Release of PHI form (see Related Links) must be obtained before PHI may be disclosed to any third party, including a business associate, in exchange for any direct or indirect remuneration, for any communication that constitutes marketing of the third party’s product or service. For example, UC may not sell or give PHI or patient lists to a third party or business associate for the third party’s own purposes.

2. Marketing Authorization Not Required
   A. During face-to-face encounter: A UC health care provider may discuss products or services of UC or a third party in a face-to-face encounter with an individual. For example, it is permitted for a health care provider to recommend a particular service or place to obtain treatment when speaking with the patient.
   B. Promotional gift of nominal value: It is permitted to give a patient or individual a promotional gift of nominal value such as a pen, magnet or calendar.
   C. Communications about UC’s products and services: It is permitted to send communications to patient or individual using PHI about products or services provided by UC. A communication about a UC product or service is not marketing under the privacy regulations. For example, it is not marketing to send information to patients to advise them of a new program offered by the UC.
   D. Communications that do not involve PHI: If the communication does not involve the use of PHI, it is permissible. For example, it is permitted to send a communication to everyone in a specific ZIP code. A communication about UC services sent to a specific population base is not marketing under the privacy regulations.
   E. Communications for case management or care coordination: It is permitted to make communications to recommend alternative treatments, therapies or health care providers or settings of care to the patient. Case management information and care coordination are not marketing under the privacy regulations.
   F. Communications about treatment: It is permitted to communicate directly with a patient about treatment tailored to the needs of the patient. A communication about treatment is not marketing under the privacy regulations.
G. Population-based communications about treatment alternatives: It is permitted to communicate with individuals about wellness and preventive medicine programs. The population may be tailored, for example, to women or a certain demographic group. A communication about a treatment alternative is not marketing under the privacy regulations.

**Related Documents**

*Authorization for the Release of PHI form*

**Benefits Plan Use and Disclosure of Protected Health Information**

1. The Benefits Plan may use and disclose PHI for the following purposes:
   A. Treatment: The Benefits Plan may disclose PHI for treatment purposes. Treatment disclosures may be made to healthcare providers that provide care to the plan members.
   B. Payment: The Benefits Plan may disclose PHI for payment purposes. Payment activities include determination of eligibility or coverage, claims processing, billing, obtaining and payment of premium, utilization review, medical necessity determinations and pre-certifications.
   C. Healthcare Operations: The Benefits Plan may disclose PHI for healthcare operations purposes.
   D. To the Plan Sponsor: The Benefits Plan may disclose summary health information to UC as the plan sponsor in order to obtain bids for health insurance coverage.
   E. Avert a Serious Threat to Health or Safety: The Benefits Plan may disclose PHI about a member when necessary to prevent or lessen a serious threat to the members’ health and safety or the health and safety of the public or another person.
   F. Military and Veterans: The Benefits Plan may disclose PHI about a member who is or was a member of the armed forces to military command authorities as authorized or required by law.
   G. Research: The Benefits Plan may use and disclose PHI for research purposes. Any disclosures for research are subject to authorization or IRB waiver of authorization requirements.
   H. Workers’ Compensation: The Benefits Plan may release PHI about a member for workers’ compensation for benefits determination.
   I. As Required by Law: The Benefits Plan may release PHI for any purpose required by law.
   J. Subject to Legal or Administrative Proceedings: The Benefits Plan may release PHI if required to do so by a court or administrative ordered subpoena or discovery request.
   K. To the Employer: The Benefits Plan may release PHI to a member’s employer if it provided healthcare at the employer’s request.
2. The Benefits Plan must deliver a Notice of Privacy Practices (NPP) to its members when benefits begin, upon request and every three years thereafter. The NPP must be prominently displayed on the Benefits Plan website.

3. Benefits Plan employees must keep separate the Benefit Plan functions from other functions not associated with the Benefits Plan such as human resources. HIPAA prohibits the use of Benefits Plan information for employment related purposes.

4. Minimum Necessary: Benefit Plan uses and disclosures are subject to the minimum necessary standard. The uses and disclosures must use the minimum amount of PHI necessary to accomplish the purpose. See Minimum Necessary Policy Statement.

Related Documents
UC Benefits Plan Notice of Privacy Practices

Disclosures to Family and Friends

1. At Time of Registration: At the time of registration for services and at other times as necessary during treatment, inform the individual that it may be necessary to share their PHI with relatives, friends, or others involved in their care or payment for care. Written notice of the practice is provided in the Notice of Privacy Practices distributed to each individual when they register for the first time in a UC health service area. The individual’s approval of this practice must be obtained unless one of the exceptions applies which allow notification for emergency or notification purposes (see numbers 3 and 4 below). Persons to whom PHI may be disclosed include a family member, other relative, or a close personal friend or any other person identified by the individual.

2. Individual is present prior to making disclosure and capable of making decisions: In this instance, obtain the individuals agreement prior to making the disclosure of PHI. If the individual has not asked the family member or friend to stay while the healthcare worker is present prior to disclosing PHI the individual should be asked for permission before disclosing PHI or ask the visitor to step out of the room.

3. Disclosure of sensitive protected health information: Federal and state law give heightened protection to certain PHI. Individual consent should not be inferred before disclosing HIV, substance abuse or mental health PHI. Before making a disclosure of sensitive PHI the individual must be asked if medical information medical information may be discussed with the family or visitor present. Alternatively the family or visitor should be asked to step out of the room. The individual should be given the opportunity to respond affirmatively before proceeding with disclosure.
4. Individual is not present, or does not have the opportunity to agree or object to the disclosure due to incapacity or emergency: A decision should be based on professional judgment as to whether the disclosure of PHI is in the best interest of the individual. If so, only the amount of information relevant to the person's involvement with the individual's health care should be disclosed.

5. Use and disclosure of PHI for notification purposes: UC may use or disclose PHI to notify a family member, legal representative, or another individual involved in the individual’s care of the individual’s location, general condition, or death.

6. Documentation of Disclosures to Family and Friends: UC is not required to document such disclosures or list them in an accounting requested by the individual.

7. PHI Disclosures Limited by Applicable State Law or Other Federal Law: Federal law or state statute more protective of PHI or that grants the individual greater rights of access to their PHI pre-empts HIPAA.
   A. Federal law or state statute may prohibit the disclosure of certain PHI without the individual's written authorization. Ohio statute, O.R.C. § 3701.243 (A) and (B) limit disclosure of HIV and AIDS related information. A signed authorization is required except for disclosures required by law.
   B. Mental health information is subject to Ohio statute, O.R.C. § 5122.31 (A) and requires individual authorization except for disclosures required by law.
   C. Federal statute 42 C.F.R. Part 2 and O.R.C. § 3719.13(B) limits disclosure of substance abuse records to third parties only with written individual authorization.
   D. Psychotherapy Notes: Information involving psychotherapy notes will not be released or disclosed to family members or friends under this policy without specific authorization by the individual.

**Decedents**

A. HIPAA protects the health information of deceased individuals for a period of 50 years. However, this does not mean that UC must retain the information for this length of time. UC may disclose protected health information about a decedent to a family member, or other person who was involved in the individual’s health care or payment for care prior to the individual’s death, unless doing so is inconsistent with any prior expressed preference, known to UC, of the deceased individual. UC may disclose PHI to coroners and medical examiners for the purpose of identifying a deceased person, determining cause of death or other duties authorized by law. UC may disclose PHI to funeral directors as necessary to carry out their duties to the decedent.
This Appendix covers procedures for assuring individuals' rights under HIPAA.

**Request for Restriction of Protected Health Information**

1. **Request for Restrictions:** UC’s Notice of Privacy Practices advises individuals of the right to request a restriction on the use and disclosure of PHI for treatment, payment, or health care operations, including the right to restrict disclosures to family members and friends involved in the individual’s care. The request for a restriction must be made by completion of the *Request for Restriction on Uses and Disclosures of PHI* form in Related Links.

2. **Approving Restrictions:** UC is not required to agree to the restriction request but will attempt to accommodate reasonable requests whenever possible. When a restriction is agreed to documentation must be made in the medical record and if the approval is not communicated to the individual orally it must be made in writing on the *Approval of Request for Restriction on Uses and Disclosures of PHI* form. A request for restriction will be evaluated by the appropriate UC Department HIPAA Coordinator and/or medical professional who may grant or deny the restriction based on their professional judgment. UC may refuse to restrict uses and disclosures or may agree only to certain aspects of the request if there is concern for the quality of individual care in the future. UC retains the right to terminate an agreed to restriction if it believes such termination is appropriate.

3. **Denying Restrictions:** If a requested restriction is not agreed to, the individual must be informed of the decision. When the restriction request is denied the UC Department HIPAA Coordinator will send the individual notification in writing on the *Denial or Termination of Request for Restriction of Use or Disclosure of Protected Health Information* form in Related Links.

4. **Agreed to Restrictions:** If a restriction is agreed to, no use or disclosure of the individual’s PHI may be made in violation of that restriction with the following exceptions:
   - **A.** When the individual who asked for the restriction is in need of emergency treatment and the restricted information is needed to provide treatment. If the information is disclosed to another health care provider for emergency treatment, request that the provider not further use or disclose the information. This request may be made orally.
   - **B.** No restriction is valid to prevent necessary disclosures to the Secretary of the U.S. Department of Health and Human Services for compliance and investigation purposes.
C. No restriction is valid for any use or disclosure that is required to be made without authorization by the individual.

5. Termination of Agreed to Restriction by UC: In the event of a termination by UC, notice of the termination will be made in writing to the individual who requested the restriction on the Denial or Termination of Request for Restriction of Uses and Disclosures of PHI by the UC Department HIPAA Coordinator. The termination notice will be added to the medical record. Only PHI that is created or obtained after the termination may be used or disclosed without the restriction after the individual is informed of the termination of the restriction. PHI created or obtained before the notification must continue to be used and disclosed consistent with the restriction.

6. Termination of Agreed to Restriction by the Individual: The individual may terminate an agreed upon restriction in writing. The written termination documentation must be attached to the medical record.

7. Business Associates: Business Associates of University of Cincinnati who may use or disclose individual PHI must be notified of any agreed-to restrictions and of any termination of an agreed-to restriction.

**Related Documents**

Request for Restriction on Uses and Disclosures of PHI form  
Approval of Request for Restriction on Uses and Disclosures of PHI form  
Denial or Termination of Request for Restriction of Uses and Disclosures of PHI

**Confidential Communications**

1. Request for Confidential Communication Form: An individual requesting confidential communications must submit the request in writing on the Request for Confidential Communications form. The individual is not required to provide an explanation for his/her request in order for UC to determine if the request is reasonable. The Request for Confidential Communications form informs the individual that if UC is unable to contact him/her using the agreed upon communication method, it will resume communications at the regular home address and telephone number.

2. Upon receipt of request for confidential communications: A determination should be made whether the request is reasonable and if it is signed by the individual or individual’s legal representative. If the request is approved, the individual should be notified that the request will be accommodated. If the request is approved and the individual is present, approval may be oral. If the individual is not present, send approval in writing on the Approval or Denial of Request for Confidential Communication form. Reasonable requests must be accommodated.
3. If the request cannot be accommodated: When a determination is made that the request for confidential communication cannot be accommodated notify the individual orally at the time of the request if present, or in writing if the individual is not present on the Approval or Denial of Request for Confidential Communication form. UC may grant an accommodation based on information the requesting individual provides regarding how payment of the bill will be handled if it is delivered to an alternative location.

4. If the request is approved: All requests that are approved must be documented in the individual’s record so that any UC employee that needs to contact the individual has access to the approved manner of confidential communication.

**Related Documents**
- Request for Confidential Communications form
- Approval or Denial of Request for Confidential Communication form

**Access to Protected Health Information**

1. Access Request: The authorized requestor may request to view PHI that is maintained electronically or to receive a copy of PHI. The authorized requestor must fill out the Individual Request to Access PHI form.

2. Response Time: When a written request for access to PHI is received, and the PHI requested is accessible on-site it must be sent out within 30 days from receipt of the request. If the request is to view PHI in electronic format or paper records an appointment should be made with the requestor to view records within 30 days. If the PHI is not accessible on-site the information must be available to view or sent within 60 days. Except as provided below, if the PHI is available and sent within 30-days of receipt of access request the individual requesting access does not require any further notice. If the PHI is stored off-site and will require 60 days or longer for UC to retrieve, the authorized requestor may be sent the Notice of Status of Individual Request for Access to PHI / Extension form

3. 30-Day Extension: A one-time 30-day extension is allowed if UC is unable to make the PHI available to the authorized requestor within the 30-day or 60-day time limit. A Notice of Status of Individual Request for Access/PHI Extension form must be sent to the authorized requestor before the original 30 or 60 days have lapsed. The extension must inform the authorized requestor the reason for the extension and the date by which UC intends to respond.
   A. Initial Action: When a written request for access is received, it must be kept with the paper or electronic medical record. Information on the request must be entered on the Individual Access to PHI Request Control Log (Attachment 3) kept in the department that creates and maintains the record. To the extent possible, grant the authorized requestor access to
the PHI sought after excluding or redacting the PHI for which there is a
ground to deny access.

B. Grounds to Deny in Whole or Part: If, after review of the request, any of
the following circumstances exist, the request should be reviewed by the
Privacy Officer who will assist with determination. A denial may be in part
or in total, as appropriate, and noted accordingly on the access log:

   i. When the keeper of the medical records performs review of the
      request for access and finds errors in the manner the form was
      completed which may cause a denial, the authorized requestor may
      make the changes necessary to allow access.
   ii. Part or the entire access request relates to a record that is not
       maintained by UC.
   iii. Part or the entire access request relates to information or a record
       that is not part of the individual's medical record.
   iv. Part or the entire access request relates to psychotherapy notes.
   v. Part or the entire access request relates to information that has
      been compiled in anticipation of or for use in a civil, criminal, or
      administrative proceeding.
   vi. Part or the entire access request relates to information created or
       obtained by UC in the course of research still in progress that
       includes treatment of the individual and the individual agreed to the
       denial of access when consenting to participate in the research.
   vii. A licensed health care professional, usually the requestor's primary
        physician and creator of the record has determined that part or all
        of the access requested by the authorized requestor is likely to
        endanger the life or physical safety of the individual or another
        person.
   viii. Part or the entire access request relates to information that makes
        reference to another person (unless such other person is a health
        care provider) and a licensed health care professional has
        determined that the access requested is reasonably likely to cause
        substantial harm to such other person.
   ix. The request is made by an inmate of a correctional institutional to
       receive a copy of the information (an inmate may not receive a
       copy but does retain the right to inspect the information).
   x. Part or the entire access request relates to information obtained by
      UC from other parties under a promise of confidentiality and access
      would likely reveal the source of the information.
   xi. Any other reasons specified by law. The Privacy Officer will provide
       HIPAA Coordinators with a list of laws that must be taken into
       account.

4. Completing the Individual Access to PHI Approval/Denial Notice: After review
and within the applicable response times defined above, an Individual Access to
PHI Approval/Denial Notice is sent to each individual requesting access. A copy
of Statement of Rights When Access to PHI is Denied must be sent to each
requestor along with the attached Request for Review of Access to PHI Denial when access to PHI is denied.

5. Providing the Information: When access is approved, the access requested should be provided in the form or format requested by the individual whether the request is to review PHI at UC or receive a copy. The individual (except for inmates) has the right to receive a copy. The individual (including inmates) also has the right to come in and inspect the medical record. The authorized requester will not be allowed to make their own copies of PHI from UC medical records.

6. Request for Review: If access is denied by a licensed health care professional under section B (7) above and the individual has been sent the Individual Access to PHI Approval/Denial Notice, the individual is entitled to a review of the denial decision. The requester may file a Request for Review of Access to PHI Denial. Assignment of the review will be made by the Privacy Officer to a different licensed health care professional not involved in the original denial decision. The reviewer will be sent the Individual Request to Access PHI form and any other information relevant to the request and the denial. The reviewer will provide a written decision within 30 days, if possible, of the receipt of the information.

7. Notice of Access to PHI Review Decision: Once the licensed health care professional reviewer has made a determination, provide notice to the individual with the Notice of Access to PHI Review Decision and note this on the access log. The individual is not entitled to any further review.

**Related Documents**
- Individual Request to Access PHI Form
- Statement of Rights When Access to PHI is Denied
- Request for Review of Access to PHI Denial
- Notice of Access to PHI Review Decision

**Amendment of Protected Health Information**

1. Request for Amendment: Written notice of the right to request amendment to PHI is given in the Notice of Privacy Practices. The request must be made in writing on Amendment of PHI Request form (see Related Links). It must specify in detail the amendment desired along with the record type, date, and location. If the requestor is aware of any other person or entity that may have a copy of the medical record they seek to have amended, they must provide that information.

   A. Timing: UC must act upon a request for amendment and respond within 60 days of receipt of the request. Note the date that the request for amendment is received. Efforts should be made to assist authorized requestor with the request so that the forms are correctly filled out and
denial is not for reasons such as lack of signature or information related to legal representative’s scope of authority to act for individual.

B. Extension: If UC is unable to grant or deny the request for amendment within 60 days, a one-time 30-day extension is allowed. The individual making the request must be provided with the reason for the extension on the Notice of Extension of Time to Answer Request for Amendment to PHI form.

C. Initial Review: The Request for Amendment does not require approval in every circumstance. The UC reviewer is the physician or licensed health care professional that created the medical record. The UC reviewer must review the request along with the medical record. The request may be denied if:
   i. The Request for Amendment relates to a record that was not created by UC. The reviewer will determine if the request to amend applies to the medical record created by the UC.
   ii. The Request for Amendment relates to information or a record that is not part of the medical record.
   iii. The Request for Amendment relates to psychotherapy notes, records compiled in anticipation of litigation, or for use in civil, criminal, or administrative proceedings.
   iv. The UC reviewer has determined that the medical record is accurate and complete.

2. Approval: When UC approves the amendment requested an Amendment of PHI Request Approval Notice (see Related Links) will be sent to the requestor along with a copy of the amended record.

3. Denial: When the request for amendment is denied, the requestor must be sent an Amendment to PHI Denial Notice (see Related Links) within 60 days of request for amendment unless an extension was requested by entity. The denial notice must contain the reason for the denial.

4. Statement of Disagreement: When an amendment request is denied the individual has the right to submit a written statement of disagreement. The statement of disagreement must be placed in the medical record.

5. Rebuttal: The UC reviewer with authority to deny the Request for Amendment has the right to make a rebuttal response to the statement of disagreement. The rebuttal must be sent to the individual and a copy placed in the medical record.

6. Future Disclosures of the Medical Record: If a statement of disagreement has been filed by the individual, future releases of the medical record will include: the Amendment to PHI Request Form, Amendment of PHI Denial Notice, the individual’s statement of disagreement, if any, and the entity rebuttal response to the statement of disagreement, if any. If no statement of disagreement was filed by the individual, the Request for Amendment and Amendment of PHI Denial
Notice (see Related Links) must be included in future releases of the record only upon request of the requestor.

7. Amendment to PHI Control Form: Amendment status, information, dates, and any amendments sent to business associates must be tracked on the Amendment to PHI Control Form (see Related Links).

Related Documents
Amendment of PHI Request form
Notice of Extension of Time to Answer Request for Amendment to PHI form
Amendment of PHI Request Approval Notice
Amendment to PHI Denial Notice
Amendment to PHI Control Form

Accounting of Disclosures of Protected Health Information

1. Requests for an Accounting: All requests for an accounting must be submitted in writing on the Request for Accounting of Disclosures of Protected Health Information form (see Related Links) and signed by an authorized requestor. The identity of the authorized requestor should be verified, as well as their authority to act on behalf of the individual if applicable. If the request form does not specify a period of time for the accounting, the accounting should include all applicable disclosures between the date of receipt and the preceding 6-year period.

   A. Response Time: When a written request for an accounting is received the accounting must be provided within 60 days of request receipt. If unable to process an accounting request within the required 60 days, a one time 30-day extension is allowed. The authorized requestor must be notified of the extension in writing with the Notice of Status of Request for an Accounting of PHI Extension form and the notice must be sent before the original 60 days have lapsed. The notice must contain the reasons for the extension and the date by which UC intends to respond.

   B. Fees: If the individual making the request for the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, provide notice to the individual that a fee for processing will be charged using either the Notice of Fee For An Accounting of Disclosures of Protected Health Information (PHI) form (see Related Links) or verbal notice and provide the requestor a chance to withdraw the request.

2. Business Associates: The accounting must include all applicable disclosures made by UC and its business associates. When an accounting request is received, each business associate will be sent a copy of the Business Associate Accounting Request form (see Related Links) within five days of the receipt of the accounting request.
3. Content of the Accounting: The accounting must include disclosures (but not uses) of the requesting individual's PHI made by UC and its business associates during the period requested by the individual up to six years prior to the request.

   A. The following types of disclosures do not have to be included in the accounting:
      i. Disclosures to carry out treatment, payment and health care operations;
      ii. Disclosures made to the authorized requestor;
      iii. Disclosures made to persons involved in the individual’s care or notification of next-of-kin or family members;
      iv. Disclosures made to UC legal counsel in the event of medical malpractice action instituted against UC by individual or individuals’ legal representative;
      v. Disclosures for national security or intelligence purposes;
      vi. Disclosures to correctional institutions or law enforcement officials about inmates or others in custody; and

   B. The accounting must include the following information for each reportable disclosure of the individual’s PHI:
      i. The date of disclosure;
      ii. The name of the entity or person to whom the information was disclosed;
      iii. If available, the address of the entity or person to whom the information was disclosed;
      iv. A brief description of the PHI disclosed; and
      v. A brief statement explaining the purpose for the disclosure.

4. Temporary Suspension Statement: It is not necessary to list within the accounting disclosures for which there is a temporary suspension statement from a health oversight agency or a law enforcement official. In order for these disclosures to be excluded, there must be a written or oral statement from the agency or official stating that providing notice of the disclosure to the individual would be reasonably likely to impede the agency’s activities and which includes a time when the suspension will be in effect. If the statement is oral, the statement must be documented, including the identity of the agency or official making the statement. If a written follow-up statement is not received within 30 days of the oral statement, the fact of the disclosure must be provided to the individual at the end of the 30 days. In all cases, the fact of the disclosure must be provided to the individual at the conclusion of the suspension period.

5. Multiple Disclosures: If there have been multiple disclosures of an individual's PHI for any purpose that does not require authorization or for which they authorized multiple disclosures to parties, the following information may be listed instead of listing each instance:

   A. For the first disclosure, all of the information listed above is required (date, name of entity, etc.).
In the event a UC employee becomes aware of a suspected or actual breach of unsecured PHI they must notify their manager and UC Department HIPAA Coordinator immediately. The UC Department HIPAA Coordinator must notify the UC Privacy Officer of a suspected breach. The UC Privacy Officer will investigate and log all the disclosures that are reportable to the Secretary, Office for Civil Rights. The report will be made to the OCR by the Privacy Officer as required by the regulations. The UC Privacy Officer will provide notification to the individual(s) that are the subject of the breach.

1. Individual Notice: UC must notify affected individuals following the discovery of a breach of unsecured PHI. UC must provide this individual notice in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically. If UC has insufficient or out-of-date contact information for 10 or more individuals, UC must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If UC has insufficient or out-of-date contact information for fewer than 10 individuals, UC may provide substitute notice by an alternative form of written, telephone, or other means.

   a. Timing of Notice: These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what UC is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for UC. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact UC to determine if their PHI was involved in the breach.

2. Media Notice: If UC experiences a breach affecting 500 or more residents of a state or jurisdiction in addition to notifying the affected individuals, it is required to
provide notice to prominent media outlets serving the state or jurisdiction. UC may provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, 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.

3. Notice in Urgent Situations: In any case determined to be urgent because of possible imminent misuse of unsecured PHI, UC may provide notification information to individuals by telephone or other means, as appropriate in addition to the written notice.

4. Law Enforcement Delay of Notification: If law enforcement informs UC that notification would impede a criminal investigation or risk national security UC shall delay notification for the time period specified by law enforcement. Notification shall not be delayed more than 30 days unless instructed in writing by law enforcement.

5. Notice to the Secretary, OCR: In addition to notifying affected individuals and the media (where appropriate), UC must notify the Secretary of breaches of unsecured PHI. UC Privacy Officer will notify the Secretary by visiting the OCR web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, UC 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, UC 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 were discovered.

6. The UC Privacy Officer will make the yearly report to the Secretary of breaches that affect less than 500 individuals within 60 days of the end of the calendar year.

7. The UC Privacy Officer will report to the Secretary without unreasonable delay any breaches that affect 500 or more individuals. The Privacy Officer will implement the process for media notice with the Public Relations department.

8. Notification by a Business Associate: If a breach of unsecured PHI occurs at or by a business associate, the business associate shall provide UC with the identification of each individual affected by the breach as well as any information required to be provided by UC in its notification to affected individuals. The business associate must contact UC within 14 business days of obtaining knowledge of a breach.

Privacy Complaints

1. Making a Privacy Complaint: Any individual who believes that their privacy has been violated by a UC covered component may make a privacy complaint to the
UC Privacy Officer or to the manager of the area involved or UC Department HIPAA Coordinator by filling out a *Privacy Complaint form* (see *Related Links*). Privacy complaints may also be conveyed verbally or by email. The manager that receives the complaint is responsible for filling out the *Privacy Complaint Intake form* (see *Related Links*). An individual has the right to make the complaint in writing to the Secretary, Department of Health and Human Services, Office for Civil Rights (OCR) by filing their complaint online at [www.hhs.gov/ocr/privacy/](http://www.hhs.gov/ocr/privacy/). Complaints may be sent to the UC Privacy Officer at University of Cincinnati, P.O. Box 0623, Cincinnati, OH 45221-0623.

Investigation: An impermissible use or disclosure of protected health information is presumed to be a breach unless UC or its business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment. HIPAA Coordinators should contact the Director of Privacy upon learning of an impermissible use or disclosure and a risk assessment shall be completed by the Coordinator and the Director as indicated within 30 calendar days of discovery. Breach notifications shall be made within 60 calendar days of discovery of the breach.

2. **Documentation of Privacy Complaints:** Each UC Department HIPAA Coordinator must document all privacy complaints received and their disposition. Records must be kept using the Privacy Complaint Intake Form. Documents must be retained for six years.

3. **No Retaliation for Making a Privacy Complaint or Filing a Complaint with the OCR:** UC may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals who make a privacy complaint to UC or the OCR.

*Related Documents*

Privacy Complaint form
Privacy Complaint Intake form
University of Cincinnati (UC) is legally required to provide you with a copy of its NOTICE OF PRIVACY PRACTICES the first time you receive care at UC. If you are here for emergency medical treatment, you will be given a copy as soon as possible.

**Patient or patient’s legal representative:**

*Please check appropriate box and sign.*

- [ ] I have received a copy of the Notice of Privacy Practices.
- [ ] I have previously received a copy of the Notice of Privacy Practices.
- [ ] I do not want a copy of the Notice of Privacy Practices.

______________________________  ________________________
Patient / Legal Representative*     Date

*Legal relationship to patient

Below this line is for UC employees’ use only if patient or patient’s legal representative has not acknowledged above.

**UC Employees:**

*Check appropriate box and sign.*

- [ ] Patient or Patient’s Legal Representative refused to sign Acknowledgement.
- [ ] Patient or Patient’s Legal Representative is unable to sign Acknowledgement.
- [ ] Patient or Patient’s Legal Representative has previously acknowledged receipt of Notice of Privacy Practices.

______________________________  ________________________
UC Employee     Date
Amendment to Protected Health Information Control

Last Name

First Name

Middle

Maiden

MRN

Date of Birth

Last 4 digits of SS#

☐ Request made by individual.

☐ Request made by individual’s personal representative.

Date Amendment Request received

Amendment Request reviewed by

Date

Request for Amendment Approved

Amendment Request received by:

☐ Mail

☐ Hand-delivery

☐ Other (specify)

Amendment made to (document which record was amended and manner in which amendment made):

Copies of amendment sent to (document names/addresses/date of those persons who have received copies of the amended information; this would include those persons identified by the individual on the amendment request form and also any business associates or other organizations that have copies of the PHI):

Amendment to PHI Control
Request for Amendment Denied

Notice of Amendment Denial sent on: ________________________________

Date Extension Notice sent: ________________________________

Reason for Denial:

☐ The authorized requestor did not include a reason for the amendment in the request form.

☐ The requested record for amendment was not created by UC.

☐ The requested record is not part of the individual's designated record set.

☐ The record is accurate and complete without the amendment.

☐ The authorized requestor is not entitled to access the record.

☐ The authorized requestor has submitted a statement of disagreement.

☐ UC has prepared a rebuttal statement.

☐ The authorized requestor has requested that the Request for Amendment and Amendment Denial Notice be included in future disclosures of the medical record.

The following has been appended to the applicable record:

________________________________________

Note: Attach the Request for Amendment to the individual record; Individual’s Statement of Disagreement, if submitted; and Rebuttal Statement, if any.

________________________________________

UC Department HIPAA Coordinator Date
UC has received your request for restriction on uses and disclosures of Protected Health information (PHI)

☐ Your request has been approved UC

agrees to the following restriction:

☐ Other

UC Department HIPAA Coordinator

Date
Authorization for Release of Protected Health Information

Last Name       First Name       Maiden

Address        City         State        Zip

Date of Birth     Last Four Digits of SS#       Phone

COPIES SENT TO

Agency/Hospital

Name of Recipient       Title

Address        City         State        Zip

PROTECTED HEALTH INFORMATION (PHI) TO BE USED OR DISCLOSED

Check box to indicate PHI that may be used or disclosed:

Dates of Treatment ____________________________:

Pertinent summary documents from the above visits will be sent, unless specified reports are indicated below:

- Face sheet*
- History & Physical
- Consultation Reports*
- Test Reports*
- Emergency Treatment
- Lab Reports*
- X-Ray Reports*
- Diagnostic Images
- Therapy Reports
- Other ____________________________
**REASON NEEDED**

Please specify the reason for your request:

- Medical care
- Disability
- At my request / personal reasons
- Legal reasons
- Insurance
- Other

I understand that if the person/entity that receives the above PHI is not a health care provider/health plan covered by federal privacy regulations, the PHI described above may be redisclosed by such person/entity and will likely no longer be protected by the federal privacy regulations.

I understand that I/my legal representative may revoke this authorization in writing at any time, except to the extent that action has been taken in reliance on this authorization. Written revocation must be sent to the University of Cincinnati Privacy Officer, P.O. Box 0623, Cincinnati, OH 45221-0623.

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits, unless the treatment is for research purposes or unless the provision of treatment is related solely to the disclosure of my PHI to a third party such as when requested by my employer.

**EXPIRATION**

This authorization will expire in 60 days unless otherwise specified (insert date or specific event):

I hereby authorize the use of disclosure of my PHI as described above. I authorize UC to release the PHI concerning treatment, diagnosis, or testing of drug or alcohol abuse, drug-related conditions, alcoholism, psychiatric/psychological conditions, Acquired Immune Deficiency Syndrome (AIDS), and/or test for antibodies to the AIDS virus (HIV).

Signature of authorized requestor* Date

*Reason patient is unable to sign

*Describe scope of authority to act for patient (provide guardianship, executor of estate, power of attorney documents):

UC Department HIPAA Coordinator Date

Retain original copy in Medical Records. Provide a copy to authorized requestor.
As a business associate of University of Cincinnati (UC) you are obligated pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations on privacy and confidentiality, 45 C.F.R. Parts 160 and 164, to maintain records of disclosures made by you of protected health information (PHI) that you have received on UC patients. Our contract with you requires the following:

Business Associate shall keep a record of disclosures of PHI and agrees to make information regarding disclosures of PHI available to UC within 15 days of a request by UC. Business Associate shall provide, at a minimum, the following information:

1. The date of disclosure;
2. The name of the entity or person who received the PHI and the address of such entity or person, if known;
3. A brief description of the PHI disclosed;
4. A brief statement regarding the purpose and explanation of the basis of such disclosure; and
5. The names of all individuals whose PHI was disclosed.

As required by contract, please submit the record of disclosures of PHI for within 15 days of receipt of this letter.

Insert period for which the accounting is requested

Further specifications:

If no disclosures were made, please notify UC in writing within 15 days.
This Data Set Agreement, effective ____________ (“Effective Date”) is entered into by and between University of Cincinnati (UC) located at ______________________________ and ____________________ (“Recipient”) located at ______________________________.

Recipient has requested permission of UC to access certain information in the form of a Limited Data Set maintained by UC for the following purpose:

The use of the Limited Data Set is for (check applicable box):

☐ Research

☐ Public health studies performed by ______________________________

☐ Health care operations of ______________________________

Name of covered entity

Description of the health care operations:

Recipient agrees to all of the following:

A. Recipient will not use or further disclose the Limited Data Set other than as permitted by this Agreement or as otherwise required by law;

B. Recipient will use appropriate safeguards to prevent the use and disclosure of the Limited Data Set other than as provided for by this Agreement;

C. Recipient will report to UC any use or disclosure of the Limited Data Set not provided for by this Agreement of which the Recipient becomes aware;

D. Recipient will ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to Recipient with respect to the Limited Data Set; and
E. Recipient will not attempt to identify the individuals whose information is in the Limited Data Set or attempt to contact the individuals.

UC reserves the right to terminate Recipient’s use of the Limited Data Set at any time that UC has reason to believe that Recipient has violated any of the conditions set forth above or has accessed any information not described herein for any purpose not described in this Agreement.

________________________________________  __________________________
Recipient of Limited Data Set                             Date

________________________________________  __________________________
UC Department HIPAA Coordinator                             Date
Denial or Termination of Request for Restriction on Uses and Disclosures of Protected Health Information

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Middle</th>
<th>Maiden</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>City</th>
<th>State</th>
<th>ZIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DENIAL OF REQUEST FOR RESTRICTION**

University of Cincinnati (UC) has received your request for restriction on uses and disclosures of Protected Health information (PHI) on

Date

☐ Your request for restriction on use or disclosure of PHI has been denied  ☐ Use or disclosure is necessary for treatment, payment or health care operations  ☐ Use or disclosure is required by law  ☐ Other

__________________________________________  ________________________________________
UC Department HIPAA Coordinator Date

**TERMINATION OF AGREED TO RESTRICTION**

UC agreed to the following restriction of uses and disclosures of your PHI on:

Date

__________________________________________  ________________________________________
UC Department HIPAA Coordinator Date

As of ________________, UC is terminating the above restriction. This termination is effective with respect to PHI created or received after the termination date.

__________________________________________  ________________________________________
UC Department HIPAA Coordinator Date
The information contained in this facsimile transmission is confidential and intended only for the use of the individual or entity named above. It may contain confidential patient health information protected by state law and federal HIPAA regulations. If the reader of this message is not the intended recipient or the agent responsible for the delivery to the intended recipient, you are hereby notified that you may not review, use, disclose, copy or distribute the information in this facsimile. Use or disclosure is prohibited and/or unlawful. If you have received this communication in error, please immediately notify the sender by telephone and return the original message at the address above via US Postal Service. We will reimburse you for all out of pocket costs you incur. Thank you.
University of Cincinnati (UC) received a request for an accounting of disclosures of patient protected health information (PHI) on ___________. There is a fee of $______________ to process accounting requests when more than one request is received within any 12-month period. This is your ____________ request for an accounting since ____________. There is a charge of $______________ to process this request.

Please notify UC immediately if you wish to withdraw your request. If UC does not receive written withdrawal of request within 10 days of your receipt of this notice, your request will be processed. You may enclose your check payable to University of Cincinnati and return it with this notice.

☐ I wish to have the accounting and my fee is enclosed.
☐ I am withdrawing my request for an accounting.

Signature of authorized requestor* ___________________________ Date ____________

*Describe scope of authority to act for individual:

__________________________________________

Return to: Privacy Officer, University of Cincinnati, P.O. Box 0623, Cincinnati, OH 45221-0623
University of Cincinnati (UC) received from you a request for an accounting of disclosures of protected health information (PHI) on __________. UC is required to take action on your request within 60 days of receipt of your request unless there are reasons why we are unable to act within that time period.

**EXTENSION**

UC will require an additional 30 days to comply with your request for the following reasons:

________________________________________

________________________________________

This is to notify you that your request will be acted upon no later than ________________

________________________________________

UC Department HIPAA Coordinator

If you have questions about this notice, you may contact:

Privacy Officer
University of Cincinnati
P. O. Box 0623
Cincinnati, OH 45221-0623
<table>
<thead>
<tr>
<th>Date complaint received</th>
<th>Form of complaint:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□ Written</td>
<td>□ Verbal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complaint received by:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Mail</td>
<td>□ Telephone</td>
</tr>
<tr>
<td>□ Walk-in</td>
<td>□ Email</td>
</tr>
<tr>
<td>□ Fax</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of Complainant</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>City</th>
<th>State</th>
<th>ZIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Anonymous Complainant</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>□</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description of problem:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action required?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes</td>
<td>□ No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action taken:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Was complaint resolved?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name of person completing this form
UC values the privacy of your protected health information (PHI). If you believe that anyone at UC has inappropriately used or disclosed information about your medical or health status, please complete this form. The UC Department HIPAA Coordinator or UC Privacy Officer will review your complaint, and all reasonable efforts will be made to resolve it.

Please describe how your health information was inappropriately used or disclosed including as much detail as possible. Use additional pages if necessary.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

May we contact you if we need additional information?  □ Yes  □ No

Name

Address

City  State  ZIP

Phone

Please send your complaint to:

Privacy Officer
University of Cincinnati
P.O. Box 0623
Cincinnati, OH 45221-0623
(Name of Primary Research Investigator or Organization) (Researcher) has requested permission of UC to use certain protected health information (PHI) maintained by UC to

(Description of the purpose of the researcher’s use of the information)

The information to be used by researcher includes

(Describe information or the type of information that the researcher will be using)

Researcher will use the patient information described above from __________ to __________.

Date

Researcher represents to UC that all of the following are true and accurate:

1. The PHI used will be used solely to prepare a research protocol or for similar purposes preparatory to research;
2. The researcher will not remove any PHI from the health facility in any form, including notes, memoranda, computerized forms, or other formats; and
3. The PHI for which access is sought is necessary for the research purpose.

UC reserves the right to terminate researcher’s use of the requested information at any time that UC has reason to believe that researcher has violated any of the conditions set forth above or has addressed any information not described herein for any purpose not described herein.

Print name of Primary Research Investigator

__________________________  Date

Primary Research Investigator Signature

__________________________  Date

UC Department HIPAA Coordinator Signature
Request for Accounting of Disclosures of Protected Health Information

The following information is required to process your request.

Last Name
First Name

Middle
Maiden

Address

City
State
ZIP

Date of Birth
Last 4 of SS#
Phone

Disclosures made from ___________ to ___________

You may request a list of disclosures for any time period within the last six years. The law does not require and UC will not provide the following disclosures of PHI to be included in an accounting:

• Disclosures made to carry out treatment, payment and health care operations;
• Disclosures made to you or your legal representative;
• Disclosures made to persons involved in your care or notification of next-of-kin or family members;
• Disclosures made to our legal counsel in the event of medical malpractice action instituted against UC by you or your legal representative;
• Disclosures for national security or intelligence purposes;
• Disclosures to correctional institutions or law enforcement officials about inmates or others in custody; or
• Disclosures that occurred prior to six previous years.

We are required to take action on your request for an accounting within 60 days of the request unless you receive a statement from us that we will need a 30-day extension to comply.

There is a fee for an accounting after you have received an accounting within any 12-month period. The charge for each subsequent accounting is $___________.

By signing this form you agree to pay the fee, if applicable.

__________________________________________
Signature of authorized requestor

__________________________________________
UC Department HIPAA Coordinator

*Describe scope of authority to act for individual:

__________________________________________

__________________________________________
I request University of Cincinnati (UC) to place the following restriction(s) on the uses and disclosures of my Protected Health Information (PHI) detailed below. I understand that restrictions may only be requested for those uses and disclosures that relate to my treatment, payment or the health care operations of UC.

I understand that UC is not required to agree to my restriction request. I further understand that UC Health reserves the right to terminate an agreed upon restriction by notifying me in writing of the termination. I may terminate an agreed upon restriction in writing by sending notice to:

Privacy Officer  
University of Cincinnati  
P.O. Box 0623  
Cincinnati, OH 45221-0097-0623

Signature of authorized requestor*  Date

*Describe scope of authority to act for patient:
(Name of Primary Research Investigator or Organization) (Researcher) has requested permission of UC to use certain protected health information (PHI) maintained by UC to

(Description of the purpose of the researcher's use of the information)

The information to be used by researcher includes

(Describe information or the type of information that the researcher will be using)

Researcher will use the decedent information described above from to

Date

Researcher represents to UC that all of the following are true and accurate:

1. The use sought is solely for research on the PHI of decedents; and
2. The PHI for which use is sought is necessary for the research purposes.

UC reserves the right to terminate researcher's use of the requested information at any time that UC has reason to believe that researcher has violated any of the conditions set forth above or has accessed any PHI described herein for any purposes not described herein.

Print name of Primary Research Investigator

Primary Research Investigator Signature

Date

UC Department HIPAA Coordinator Signature

Date
I. THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The terms of this Notice of Privacy Practices (NPP) apply to University of Cincinnati (UC). The UC covered entities and licensed health care professionals will share protected health information of patients as necessary to carry out treatment, payment, and health care operations as permitted by law.

II. WE HAVE A LEGAL DUTY TO SAFEGUARD YOUR PROTECTED HEALTH INFORMATION

We are required by law to maintain the privacy of our patients' health information. This information is called Protected Health Information (PHI). We must provide our patients with notice of our legal duties and privacy practices with respect to PHI. We are required to abide by the terms of this NPP so long as it remains in effect. We reserve the right to change the terms of this NPP as necessary and to make the new NPP effective for all PHI maintained by us. You may receive a paper copy of this or any revised notices at the location where you receive your health care or you may view a copy of the notice on our website at www.uc.edu.

III. USES AND DISCLOSURES OF YOUR PROTECTED HEALTH INFORMATION

Your Authorization. We will not use or disclose your PHI for any purpose other than treatment, payment and health care operations unless you have signed a form authorizing the use or disclosure with the exception of the situations outlined below. You have the right to revoke that authorization in writing unless we have taken any action in reliance on the authorization.

Uses and Disclosures for Treatment. We will make uses and disclosures of your PHI as necessary for your treatment. For instance, doctors and nurses and other professionals involved in your care will use information in your medical record and information that you provide about your symptoms and reactions to plan a course of treatment for you that may include tests and medications.

Uses and Disclosures for Payment. We will make uses and disclosures of your PHI as necessary for payment purposes. For instance, we may forward information regarding your medical procedures and treatment to your insurance company to arrange payment for the services provided to you or we may use your information to prepare a bill to send to you or to the person responsible for your payment. We may make uses and disclosures of your PHI to another entity or health care provider for payment of the entity that receives the information.

Uses and Disclosures for Health Care Operations. We will use and disclose your PHI as necessary, and as permitted by law, for our health care operations which include clinical improvement, professional peer review, business management, etc. For instance, we may use and disclose your PHI for purposes of improving
the clinical treatment and care of our patients.

Electronic Medical Record. UC Student Health Services utilizes an electronic medical record. You have the right to receive your records that are held in an electronic medical record in that format upon request.

Family and Friends Involved In Your Care. With your approval, we may disclose your PHI to designated family, friends, and others who are involved in your care or in payment of your care in order to facilitate treatment and payment. If you are unavailable, incapacitated, or facing an emergency medical situation and we determine that a limited disclosure may be in your best interest, we may share limited PHI with such individuals without your approval.

Disaster Relief. We may also disclose limited PHI to a public or private entity that is authorized to assist in disaster relief efforts in order for that entity to locate a family member or other persons that may be involved in some aspect of caring for you.

Business Associates. Certain aspects and components of our services may be performed through contracts with outside persons or organizations. At times it may be necessary for us to provide certain of your PHI to one or more of these outside persons or organizations who assist us with our healthcare operations. In all cases, business associates are required to appropriately safeguard the privacy of your information.

Fundraising. We may contact you to donate to a fundraising effort for or on our behalf. You have the right to "opt-out" of receiving fundraising materials or communications and may do so by sending your name and address to: Privacy Officer, University of Cincinnati, P.O. Box 0623, Cincinnati, OH 45221-0623.

Please include a brief statement with your wish not to receive fundraising materials or communications from us.

Marketing. We must receive your authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of a face-to-face communication made to you personally; or a promotional gift of nominal value provided by UC. It is not considered marketing to send you information related to your individual treatment, case management, and care coordination or to direct or recommend alternative treatment, therapies, health care providers or settings of care. These may be sent without written permission. If the marketing is to result in direct or indirect payment to the UC by a third party we will state this on the authorization.

Appointments and Services. We may contact you to provide appointment reminders or information about other health-related benefits and services that may be of interest to you. You have the right to request to receive communications regarding your PHI from us by alternative means or at alternative locations. We agree to comply with reasonable requests. For instance, if you wish appointment reminders to not be left on voice mail or sent to a particular address, we will accommodate reasonable requests. You must request such confidential communication in writing and send your request to: Privacy Officer, University of Cincinnati, P.O. Box 0623, Cincinnati, OH 45221-0623.

Confidentiality of Alcohol and Drug Abuse Records. Federal law and regulations protect the confidentiality of alcohol and drug program records maintained by UC. PHI containing information on your alcohol or drug use may not be disclosed without 1) your
written authorization; 2) a court order; or 3) unless the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit or program evaluation. Federal law or regulations do not protect any information about a crime committed by you at our facility or about any threat to commit a crime. Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under state law to appropriate state or local authorities.

**Other Uses and Disclosures.** We are permitted or required by law to make certain other uses and disclosures of your PHI without your authorization.

- We may release your PHI for any purpose required by law; if we suspect child abuse or neglect; if we believe you to be a victim of abuse, neglect, or domestic violence; to law enforcement officials as required by law to report wounds, injuries and crimes; if required by law to a government oversight agency conducting audits, investigations, or civil or criminal proceedings; and if required to do so by a court or administrative ordered subpoena or discovery request; in most cases you will have notice of such release;

- We may release your PHI for public health activities, such as required reporting of disease, injury, and birth and death, and for required public health investigations; we may release your PHI to coroners and/or funeral directors consistent with law;

- We may release your PHI to the Food and Drug Administration if necessary to report adverse events, product defects, or to participate in product recalls;

- We may release your PHI to your employer when we have provided health care to you at the request of your employer; in most cases you will receive notice that information is disclosed to your employer;

- We may release your PHI if in limited instances we suspect a serious threat to health or safety;

- We may release your PHI for certain research purposes without your authorization when such research is approved by an institutional review board with established rules to ensure privacy or with researcher representation that limit the use and disclosure of the PHI;

- We may release your PHI if you are a member of the military as required by armed forces services; we may also release your PHI if necessary for national security or intelligence activities; and

- We may release your PHI to workers’ compensation agencies if necessary for your workers’ compensation benefit determination.

- Ohio law requires that we have your authorization or a court order before disclosing the results of an HIV test or diagnosis of AIDS or AIDS-related condition.
IV. RIGHTS THAT YOU HAVE REGARDING YOUR PHI

Access to Your Protected Health Information. You have the right to receive a copy and/or inspect much of the PHI we retain on your behalf in paper or electronic format, unless excluded by law. All requests for access must be made in writing and signed by you or your legal representative. We may charge you a fee for copying the information and for postage if you request a mailed copy. You may obtain an access request form from the site where you receive your care.

Amendments to Your Protected Health Information. You have the right to request in writing that PHI that we maintain about you be amended. We are not obligated to make all requested amendments but will give each request careful consideration. All amendment requests, in order to be considered by us, must be in writing, signed by you or your representative, and must state the reasons for the amendment request. If an amendment you request is made by us, we may also notify others who work with us and have copies of the uncorrected record if we believe that such notification is necessary. You may obtain an amendment request form from the site where you received your care.

Accounting for Disclosures of Your Protected Health Information. You have the right to receive an accounting of certain disclosures made by us of your PHI. Requests must be made in writing and signed by you or your legal representative. Accounting request forms are available from: Privacy Officer, University of Cincinnati, 650 University Pavilion, P.O. Box 210623, Cincinnati, OH 45221-0623.

The first accounting in any 12-month period is free; you will be charged a reasonable fee as allowed by law for each subsequent accounting you request within the same 12-month period.

Restrictions on Use and Disclosure of Your Protected Health Information. You have the right to request a restriction on the uses and disclosures of your PHI for treatment, payment and health care operations. We are not required to agree to your restriction request but will attempt to accommodate reasonable requests when appropriate and we retain the right to terminate an agreed-to restriction if we believe such termination is appropriate. In the event of a termination by us, we will notify you of such termination. You also have the right to terminate, in writing, any agreed-to restriction by sending such termination notice to: Privacy Officer, University of Cincinnati, 650 University Pavilion PO Box 210623 Cincinnati, OH 45221-0623.

Right to Restrict Disclosure to Health Plan if You Pay for Services Out of Pocket. You have the right to request a restriction and we will agree to a restriction on the disclosure of your PHI to a health plan if the disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and the PHI pertains solely to a health care item or service that you and not your health plan have paid UC for in full out of pocket.

V. HOW TO COMPLAIN ABOUT OUR PRIVACY PRACTICES

If you believe your privacy rights have been violated, you may file a complaint in writing to the Privacy Officer, University of Cincinnati, 650 University Pavilion P.O. Box 210623, Cincinnati, OH 45221-0623.

You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Office for Civil Rights, Region V, 233 N. Michigan Avenue, Suite 240,
Chicago, IL 60601 in writing within 180 days of an alleged violation of your rights. There will be no retaliation for filing a complaint.

**VI. PERSON TO CONTACT FOR FURTHER INFORMATION OR ASSISTANCE**

If you have questions or need further assistance regarding this Notice, you may contact the Privacy Officer, University of Cincinnati, 650 University Pavilion, P.O. Box 210623, Cincinnati, OH 45221-0623.

As a patient you retain the right to obtain a paper copy of this NPP, even if you have requested a copy by e-mail or other electronic means.