PRIVACY OFFICE

HIPAA POLICY MANUAL

(Effective: December 1, 2020)

PRIVACY OFFICE HIPAA POLICY MANUAL

TABLE OF CONTENTS

The scope of this policy shall include all applicable provisions of the above-referenced regulations, even if not expressly cited herein.

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**HIPAA Policies and Procedures**
Policy Number:	**PO-1**

Policy Statement

In accordance with federal regulations [45 CFR §164.530(i)] and University policy, the University of Louisville will maintain required policies and procedures to ensure the privacy, security and proper use and disclosure of Protected Health Information (PHI), in compliance with applicable federal and state law, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C).

Procedure

The Privacy Office will organize, maintain, and periodically review the University of Louisville Privacy Office HIPAA Policy Manual. The Privacy Office will periodically review and make recommendations for changes, as applicable, to the University of Louisville Administrative HIPAA Privacy Policy Management (HPR-1.01) Policy.

The Privacy Office will maintain its policy manual in written and/or electronic form. An electronic copy of the Privacy Office HIPAA Policy Manual will be available on the Privacy Office website at www.louisville.edu/privacy.

In the event of a change in the law, including the standards, requirements, and implementation specifications, of the relevant statutes and regulations, the:

A. Privacy Officer will review applicable policies and procedures to determine which policies and procedures are affected;
B. Privacy Officer may determine the need to make the changes effective for Protected Health Information created or received prior to the effective date of the notice revision;
C. Necessary revisions will be made to the University's Notices of Privacy Practices, if applicable;
D. Necessary changes to applicable policies and procedures will be documented by modifying the policy and procedure and dating the revision with the new revised effective date;

E. Workforce members of the Health Care Component of the University of Louisville will be informed of the revisions.

The University may change, at any time, a policy or procedure that does not materially affect the content of the Notices of Privacy Practices, provided that:

A. The revised policy or procedure complies with the standards, requirements, and implementation specifications of the privacy regulations; and

B. Prior to the effective date of the change, the revised policy or procedure is documented in written or electronic form.

The University shall provide and document training of its workforce members regarding any changes to the University's policies and procedures to the extent such change affects the workforce member's job responsibilities or access, use, or disclosure of PHI.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Designation of Hybrid Covered Entity Status**
Policy Number:	**PO-2**

Policy Statement

In accordance with federal regulations [45 CFR §164.105(a)], the University of Louisville has designated itself as a hybrid covered entity. As such, the colleges, schools, departments, and administrative business units which perform covered functions, or act as a business associate to a covered entity, are included in the University of Louisville's health care component of the hybrid covered entity. Colleges, schools, departments, and administrative business units within the health care component are subject to the University of Louisville HIPAA Privacy Policy (HPR-1.01) and the University of Louisville Privacy Office HIPAA Policies and Procedures.

The following areas have been designated to be within the University of Louisville health care component:

- *Campus Health Services* (*excludes the Prevention, Education, and Advocacy on Campus and in the Community (PEACC) Program and the Health Promotion Program)* - subdivision of services provided to non-students
- *Department of Athletics* - subdivision which processes the level-funded insurance plan offered to student athletes
- *Department of Audit Services*
- *Department of Environmental Health & Safety*
- *Department of Risk Management*
- *Department of University Advancement/Development* – subdivision which performs fundraising activities
- *Human Resources* - subdivisions which process employee health plan (e.g., Benefits; Total Rewards program)
- *Information Security Compliance Office*
- *Information Technology Services*

- *Office of Communications & Marketing*
- *Office of Finance/Controller* – subdivisions of the Controller's Office which process health care related payments
- *Office of University Counsel*
- *Procurement Services – ProCard staff only*
- *School of Dentistry and affiliated Institutes and Centers (includes research activities)*
- *School of Medicine (**NOTE:** excludes research activities and clinics/physician practices that are owned/operated by University of Louisville Health)*
- *University Archives & Records* – the subdivision which handles and/or stores protected health information
- *University Integrity & Compliance Office*
- *University Privacy Office*

The hybrid covered entity designation will be reviewed when new components are added or when new University-wide systems are implemented.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Designation of Privacy Officer**
Policy Number:	**PO-3**

Policy Statement

In accordance with federal regulations [45 CFR 164.530(a)], the University of Louisville has designated the University Privacy Officer to be responsible for the development and implementation of HIPAA policies and procedures of the University, for receiving and responding to privacy complaints and questions, to cooperate with the U.S. Department of Health and Human Service's Office for Civil Rights, and to provide further information about matters covered by the University's Notices of Privacy Practices.

The University Privacy Officer shall be responsible for the management and operations of the University Privacy Office.

Procedure

The University Privacy Officer shall respond to privacy complaints and questions raised as a result of the University of Louisville Privacy Office *Duty of Workforce Members to Report Privacy and Security Concerns* (Privacy Office Policy Number PO-9). Suspected breaches of Protected Health Information (PHI) shall be investigated by the University of Louisville Privacy Office and, in the event of a reportable breach, the Privacy Office shall provide response and notification as outlined in the University of Louisville Privacy Office *Breach Response and Notification* Policy (Privacy Office Policy Number PO-18).

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Confidential Question or Complaint Form

Related Information

University Privacy Office information website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Privacy & Security Compliance**
Policy Number:	**PO-4**

Policy Statement

In accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C), the University Privacy Officer and the University Chief Information Security Compliance Officer shall collaborate to ensure alignment between security and privacy compliance programs. This collaboration shall ensure the privacy, security, and proper use and disclosure of University Protected Health Information (PHI), in compliance with applicable federal and state law.

Procedure

Workforce members of the Health Care Covered Component of the UofL Hybrid Covered Entity shall comply with both the Privacy Office HIPAA Policies and Procedures and with Information Security Compliance Office Policies and Standards.

Related Information

University Privacy Office information website: http://louisville.edu/privacy

University Information Security Compliance Office website: http://louisville.edu/security

The ISO Policies and Standards are available at http://louisville.edu/security/policies. Per ISO Policy and Standard ISO-001, each member of the campus community is responsible for the security and protection of information resources over which he or she has control, including networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

U.S. Department of Health and Human Services information regarding the HIPAA Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/index.html

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**HIPAA Definitions**
Policy Number:	**PO-5**

Policy Statement

In accordance with federal regulations [45 CFR §164.530(i)] and University policy, the University of Louisville will maintain required policies and procedures to ensure the privacy, security and proper use and disclosure of Protected Health Information (PHI), in compliance with applicable federal and state law, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C).

Procedure

Breach

For purposes of the breach notification provisions of HIPAA, *breach* means the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under the privacy regulations which compromises the security or privacy of the PHI. For purposes of this definition, *compromises the security or privacy of the PHI* means poses a significant risk of financial, reputational, or other harm to the Individual.

Business Associate

A person or organization, or any subcontractor of a Business Associate, that creates, receives, maintains, or transmits Protected Health Information to perform a function or activity on behalf of the Provider, such as claims processing, claims administration, data analysis, utilization review, quality assurance, billing, practice management, legal counsel, benefits management, or information technology consultants.

Correctional Institution

Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian

tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity

A health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered Function

Those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data Aggregation

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

Designated Record Set

A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about Individuals. For purposes of this definition, the term *record* means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct Treatment Relationship

A treatment relationship between an Individual and a health care provider that is not an indirect treatment relationship.

Disclosure

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

Electronic Media

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. *Transmission media* include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information (ePHI)

Electronic Protected Health Information means Protected Health Information that is transmitted by electronic media or maintained in electronic media.

Employer

The person for whom an Individual performs or performed any service, of whatever nature, as the employee of the person, except that:

A. If the person for whom the Individual performs or performed the services does not have control of the payment of the wages for the services, the term employer means the person having control of the payment of the wages, and

B. In the case of a person paying wages on behalf of a nonresident alien Individual, foreign partnership, or foreign corporation, not engaged in trade or business within the United States, the term employer means the person.

Family Member

With respect to an Individual:

A. A dependent (as such term is defined in 45 CFR 144.103) of the Individual; or
B. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the Individual or of a dependent of the Individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents). *First-degree relatives* include parents, spouses, siblings, and children. *Second-degree relatives* include grandparents, grandchildren, aunts, uncles, nephews, and nieces. *Third-degree relatives* include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. *Fourth-degree relatives* include great-great grandparents, great-great grandchildren, and children of first cousins.

Fundraising Communications

Communications, whether written or oral, that include appeals for money, sponsorship of events, or similar support.

Genetic Information

With respect to an Individual, information about:

A. The Individual's genetic tests;
B. The genetic tests of family members of the Individual;
C. The manifestation of a disease or disorder in family members of such Individual; or
D. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the Individual or any family member of the Individual.

Any reference in the HIPAA regulations to genetic information concerning an Individual or family member of an Individual must include the genetic information of:

(i) A fetus carried by the Individual or family member who is a pregnant woman; and
(ii) Any embryo legally held by an Individual or family member utilizing an assisted reproductive technology.

Genetic information excludes information about the sex or age of any Individual.

Genetic Services

(1) A genetic test; (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) Genetic education.

Genetic Test

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. *Genetic test* does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Health Care

Care, services, or supplies related to the health of an Individual.

Health care includes, but is not limited to, the following:

A. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or

mental condition, or functional status, of an Individual or that affects the structure or function of the body; and

B. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse

A public or private entity such as a billing service, a repricing company, or management and information systems that processes Health Information received from another entity into a HIPAA-compliant transaction for the electronic transmission of that Health Information.

Health Care Component of a Hybrid Covered Entity

The Privacy Rule permits a covered entity that conducts both covered and non-covered functions to elect to be a *hybrid entity*. The activities that make an organization a covered entity are its covered functions. A hybrid entity must designate the areas within its organization that perform covered functions; these designated areas are the hybrid entity's *health care component*. After making this designation, most of the requirements of the Privacy Rule will apply only to the health care component.

Health Care Operations

Any activities of the Provider related to activities necessary to carry on business activities associated with the provision or administration of Health Care, including but not limited to activities associated with quality assurance and improvement, credentialing and license verification, practitioner and provider evaluations, insurance contracting and underwriting, audits and surveys, legal services, compliance programs, business planning and development, management and general administration.

Health Care Provider

A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Information

Any information, including genetic information, whether oral or recorded in any form or medium, that:

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

Health Oversight Agency

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

Health Plan

An Individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)). Health plan includes group health plans, health insurance issuers, approved State child health plans, the Medicare Advantage program, high risk pools established under State law to provide health insurance coverage or comparable coverage to eligible Individuals, and any other Individual or group plan, or combination of Individual or group plans, that provides or pays for the cost of medical care.

Indirect Treatment Relationship

A relationship between an Individual and a health care provider in which:

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

Individually Identifiable Health Information

Information, including demographic data, that relates to:

- the Individual's past, present or future physical or mental health or condition,
- the provision of health care to the Individual, or
- the past, present, or future payment for the provision of health care to the Individual,

and

that identifies the Individual or for which there is a reasonable basis to believe it can be used to identify the Individual.

Inmate

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

Law Enforcement Official

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

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

Manifestation or Manifested

With respect to a disease, disorder, or pathological condition, that an Individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of the HIPAA regulations, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Marketing

Any communications made about products or services with the intent to encourage Individuals to use or purchase the products or services, with certain exceptions as stated in the Privacy Rule.

Notice of Privacy Practices (NPP)

A written notice provided to an Individual by the Provider describing the Uses and Disclosures of Protected Health Information that may be made by the Provider, the Individual's privacy rights, the Provider's legal duties with respect to the Individual's Protected Health Information, and the Individual's right to file a complaint upon belief that his/her privacy rights have been violated, prepared and distributed in accordance with the requirements set forth in the HIPAA Privacy Rule.

Organized Health Care Arrangement

Any of the following five types of arrangements:

A. A clinically integrated care setting in which an Individual typically receives Health Care from more than one Health Care Provider, e.g., a hospital and its medical staff;
B. An organized system of Health Care in which more than one Covered Entity participates and the participating Covered Entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities, including at least one of the following: 1. Utilization review, performed by other participating entities or a third party on behalf of the participating entities, 2. Quality assessment and improvement activities, assessed by other participating entities or a third party on behalf of the participating entities, and/or 3. Payment activities, if the financial risk for delivering care is shared by the participating Covered Entities through the joint arrangement and if Protected Health Information created or received by a

Covered Entity is reviewed by other participating Covered Entities or by a third party on behalf of the joint arrangement for the purpose of administering the sharing of a financial risk;

C. A Group Health Plan and a health insurance insurer or HMO of the Group Health Plan, but only with respect to Protected Health Information created or received by the health insurance insurer or HMO that relates to Individuals who are or who have been participants or beneficiaries of the Group Health Plan;
D. A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same plan sponsor; or
E. The Group Health Plans described in (D) of this definition and health insurance issuers or HMOs with respect to such Group Health Plans, but only with respect to Protected Health Information created or received by such health insurance issuers or HMOs that relates to Individuals who are or have been participants or beneficiaries in any of such Group Health Plans.

Payment

Activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a Health Care provider or health plan to obtain or provide reimbursement for the provision of Health Care; for activities that relate to the Individual to whom Health Care is provided.

Protected Health Information (PHI)

Individually identifiable health information that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium.

Protected Health Information excludes Individually Identifiable Health Information:

1. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
2. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
3. In employment records held by a covered entity in its role as employer; and
4. Regarding a person who has been deceased for more than 50 years.

Psychotherapy Notes

Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public Health Authority

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

Required by Law

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

Research

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

Sale of Protected Health Information (PHI)

A disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Sale of PHI does not include a disclosure of PHI:

(i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);
(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the Protected Health Information for such purposes;
(iii) For treatment and payment purposes pursuant to § 164.506(a);
(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);
(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;
(vi) To an Individual, when requested under § 164.524 or § 164.528;

(vii) Required by law as permitted under § 164.512(a); and
(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the Protected Health Information for such purpose or a fee otherwise expressly permitted by other law.

Secretary

The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Subcontractor

A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Treatment

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

Underwriting Purposes

With respect to a health plan, *underwriting purposes* means

(1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
(2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payment in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
(3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
(4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

Underwriting purposes does not include determinations or medical appropriateness where an Individual seeks a benefit under the plan, coverage, or policy.

Unsecured Protected Health Information

Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized Individuals 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 on the HHS Web site.

Use

With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce

Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. For purposes of this definition, the University includes students as part of its workforce.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Training**
Policy Number:	**PO-6**

Policy Statement

In accordance with federal regulations [45 CFR §164.530(b)], all Workforce Members of the Health Care Component of the University of Louisville (UofL) Hybrid Covered Entity who may have access to Protected Health Information (PHI) shall receive training regarding HIPAA policies and safeguards. Such training shall be conducted upon hire, upon a change of job function as described below, and at the intervals described below as is commensurate with job duties and/or academic class level.

Procedure

All required training programs listed below may be provided via UofL's online training program or via a live training session conducted by the Privacy Office, or the Privacy Office's delegate as necessary.

HIPAA Privacy

HIPAA Privacy training is required for all members of the workforce who are assigned or employed in a college, school, department, or administrative business unit which has been designated to be within the health care component.

HIPAA Privacy training shall be provided as follows:

1. To each new member of the workforce within 30 days after the Individual joins the workforce;
2. To each workforce member who transfers from a position within UofL that did not require HIPAA Privacy training to a position within UofL which requires HIPAA Privacy training, to be completed within thirty (30) days of job change;
3. To each member of the workforce whose functions are affected by a material change in the policies or procedures required by HIPAA, within 30 days after the material change becomes effective; and
4. To all members of the workforce (who are assigned to a location within the UofL health care component) on an annual basis.

HIPAA Privacy training is effective for one (1) year.

[Note: Basics of Information Security training is provided on an annual basis as part of the Attestation and Disclosure Form (ADF)]

HIPAA Training from Previous Jobs or Experience

The University will not waive the training requirements for workforce members on the basis that HIPAA training was previously received elsewhere.

Training for Temporary or Short-Term Workforce Members

If an Individual will be part of a college, school, department, or administrative business unit's workforce for two weeks or less, the training described above is not required. In this case, the Individual will sign a *Confidentiality Agreement – Short Term Workforce Member Form,* available on the University Privacy Office website (http://louisville.edu/privacy), prior to the use or disclosure of any Protected Health Information.

The college, school, department, or administrative business unit shall provide a copy of the signed Confidentiality Agreement – Short Term Workforce Member Form to the workforce member, maintain a copy for its own records, and forward a copy to the University Privacy Office.

Enforcement

Each college, school, department, or administrative business unit shall be responsible for ensuring that workforce members have received the appropriate HIPAA training based on the workforce members' job responsibilities. The Privacy Office is responsible for oversight and enforcement of HIPAA training, in collaboration with the Department of Human Resources and the Office of the Provost, as necessary.

Training Documentation

Each college, school, department, or administrative business unit should maintain documentation of HIPAA training provided to its workforce. Such documentation should include a copy of the content that was delivered as well as: 1) The name of the Individual who received the training; 2) The date the training was provided; and 3) The topic of the content that was delivered.

Sanctions

With limited exception, the University will apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the University or the requirements of HIPAA. Any sanctions applied as a result of the failure of a workforce member to comply with the University's policies and procedures or HIPAA requirements shall be documented as required by the University's policies and procedures.

Each college, school, department, or administrative business unit must ensure that all workforce members receive and acknowledge training of UofL sanctions policy for non-compliance with privacy and security policies and regulations.

The University of Louisville Privacy Office *Sanctions* Policy (Privacy Office Policy PO-14) provides further information regarding sanctions for failure to comply with University Privacy Office Policies and Procedures.

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Confidentiality Agreement - Short-Term Workforce Member Form

Related Information

University of Louisville Department of Human Resources website: https://louisville.edu/hr/.

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name: **Job Shadowing**
Policy Number: **PO-7**

Policy Statement

The University of Louisville (UofL) Privacy Office will maintain required policies and procedures to ensure the privacy, security and proper use and disclosure of Protected Health Information (PHI), in compliance with applicable federal and state law, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C).

Procedure

UofL understands that Job Shadowing is an important part of the learning experience, especially in clinical practice areas; however, care must be taken to ensure that the University's PHI is properly safeguarded from unauthorized access, use, or disclosure.

Where a Job Shadow Participant is not affiliated with UofL, or otherwise authorized to enter the job site or clinical area, the college, school, department, or administrative business unit shall facilitate all shadow/observation activities, which includes:

A. Verifying the Job Shadow Participant's identity;
B. Determining appropriateness of objectives;
C. Assigning a staff or faculty member responsible for oversight; and
D. Ensuring the Job Shadow Participant's understanding of patient privacy and confidentiality.

The Job Shadow Participant may not actively participate in patient care.

The Job Shadow Participant must sign a Confidentiality Agreement (available on the University Privacy Office website at www.louisville.edu/privacy). A copy of the Confidentiality Agreement shall be sent to the University Privacy Office, a copy maintained in the college, school, department, or administrative business unit, and a copy provided to the Job Shadow Participant.

If the Job Shadow Participant is expected to shadow for two weeks or more, then the University's formal HIPAA training is required (see Privacy Office Policy PO-6 *Training*).

If the Job Shadow Participant is under the age of 18, please consult the UofL Minors on Campus webpage (https://louisville.edu/riskmanagement/minors-on-campus) to ensure that the proper documentation has been completed and that the Job Shadow Participant's activities do not conflict with UofL policies regarding minors on campus.

While the Job Shadow Participant is shadowing, and at the beginning of each patient encounter, the UofL personnel member responsible for oversight of the Job Shadow Participant must introduce the Job Shadow Participant to the patient, explain why the Job Shadow Participant is there, and offer the patient or the patient's legal representative the right to agree or object to the continued presence of the Job Shadow Participant. The agreement or objection may be obtained in written or verbal form.

The University personnel responsible for oversight must limit the use and disclosure of PHI to the minimum level necessary to meet the Job Shadow Participant's objectives (see Privacy Office Policy PO-10.1 *Minimum Necessary*).

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Confidentiality Agreement – Short-Term Workforce Member

Related Information

University of Louisville Privacy Office website: www.louisville.edu/privacy

University of Louisville Minors on Campus webpage: https://louisville.edu/riskmanagement/minors-on-campus

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Business Associate Agreements**
Policy Number:	**PO-8**

Policy Statement

In accordance with federal regulations [45 CFR §164.502, 45 CFR §164.504 & 45 CFR §164.532], the University of Louisville will enter into Business Associate Agreements (BAAs) to establish the permitted and required uses and disclosures of Protected Health Information (PHI).

Procedure

The University of Louisville (UofL) will allow its Business Associates to create, receive, maintain, or transmit PHI on its behalf, if UofL obtains satisfactory written assurance, via a BAA, that the Business Associate will appropriately maintain the Privacy and Security of the PHI and fulfill HIPAA Business Associate obligations.

In the event that UofL becomes aware of a pattern of an activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangement, the University will take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, UofL may terminate the contract or arrangement, if feasible.

If UofL, in the role of a Business Associate, becomes aware of a pattern of an activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the contract or other arrangement, UofL will take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, UofL may terminate the contract or arrangement, if feasible.

BAA templates provided on the University Privacy Office website (http://louisville.edu/privacy) shall be used to ensure that all of the elements required by the regulations are included. Contact the Privacy Office with questions regarding use of BAAs.

If the other party to the agreement proposes changes to the UofL BAA template or proposes use of a template of its own, the proposed BAA must be sent to the UofL Privacy Office, or the Privacy Office's delegate as applicable, for review before the BAA may be signed.

A copy of all fully signed BAAs shall be forwarded to the University Privacy Office.

Forms

The forms listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- BAA – UofL as CE
- BAA – UofL as BA
- HIPAA Subcontractor Agreement

Related Information

University Privacy Office information website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Privacy & Security Concerns**
Policy Number:	**PO-9**

Policy Statement

In accordance with the HIPAA Privacy and Security Rules, and to ensure the privacy and confidentiality of Protected Health Information (PHI), the University of Louisville (UofL) provides the means for patients to report privacy and/or security concerns. UofL requires workforce members of the Hybrid Covered Entity Health Care Component (HCC) to report all known or suspected privacy and security incidents to UofL.

Procedure

Privacy concerns, suspected breaches of PHI, or known breaches of PHI may be reported by any of the following methods:

- Contact the University Privacy Officer at (502) 852-3803 or privacy@louisville.edu;
- Contact the University Information Security Compliance Office at (502) 852-6692 or isopol@louisville.edu
- Contact the University's Compliance Hotline at (877) 852-1167;
- File a report using the University's online reporting system at http://louisville.edu/compliance/ico/hotline; or
- Confidential Question or Complaint Form.

Security concerns and issues regarding suspected breaches of electronic information should be reported to the Information Security Compliance Office at isopol@louisville.edu or via website at http://louisville.edu/security.

If a patient or community member reports to a workforce member that he/she would like to file a privacy or security complaint or concern, the workforce member should provide the patient or community member with a Confidential Question or Complaint Form or direct the patient to the Privacy Office website.

University employees are not permitted to engage in retaliation, retribution, or any form of harassment against another employee for reporting a compliance concern, ethical matter, or other questionable practice (University Policy Number ICO-1.01 and Privacy Office Policy Number PO-15 *No Retaliation*).

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Confidential Question or Complaint Form

Related Information

University Privacy Office website: http://louisville.edu/privacy

University of Louisville Policy Library: http://louisville.edu/compliance/policies.

University Information Security Office website: http://louisville.edu/security

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information**
Policy Number:	**PO-10**

Policy Statement

In accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C), it is the policy of the University of Louisville (UofL) to comply with HIPAA and to use or disclose Protected Health Information (PHI) only as permitted by the Privacy Rule and the Security Rule. Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (HCC) shall use and disclose PHI as set forth below and in all included policy subsets.

Procedure

The UofL HCC is **required** to disclose PHI:

- To the Individual who is the subject of the information requested (see Privacy Office Policy PO-20 *Individual Rights*)

- To the Secretary to investigate or determine the HCC's compliance with the privacy regulations. Disclosures made to the Secretary are required to be documented in the Accounting of Disclosures (see Privacy Office Policy PO-20 *Individual Rights*)

If the UofL HCC is functioning as a business associate, it is **required** to disclose PHI:

- To the covered entity, Individual, or Individual's designee, as necessary to satisfy a covered entity's obligations with respect to an Individual's request for an electronic copy of PHI (see Privacy Office Policy PO-20 *Individual Rights*)

- To the Secretary to investigate or determine the business associate's compliance with HIPAA.

The UofL HCC is **permitted** to use or disclose PHI as described in the following policy subsets:

- *Minimum Necessary (Policy Number PO-10.1)*
- *Verification Requirements (Policy Number PO-10.2)*
- *Treatment, Payment, and Health Care Operations (Policy Number PO-10.3)*
- *Authorizations (Policy Number PO-10.4)*
- *Authorization Required for Educational/Instructional Purposes (Policy Number PO-10.5)*
- *Personal Representatives (Policy Number PO-10.6)*
- *Uses and Disclosures Without Authorization (Policy Number PO-10.7)*
    - *Disclosures for Public Health Activities*
    - *Disclosures Regarding Victims of Abuse, Neglect, or Domestic Violence*
    - *Disclosures for Health Oversight Activities*
    - *Disclosures for Judicial and Administrative Proceedings*
    - *Disclosures to Law Enforcement*
    - *Disclosures Regarding Decedents*
    - *Disclosures to Avert a Serious Threat or Injury*
    - *Disclosures for Specialized Government Functions*
    - *Disclosures for Worker's Compensation*

- *Use and Disclosure for Research (Policy Number PO-10.8)*
    - *Uses and Disclosures of De-Identified Information*
    - *Uses and Disclosures of Limited Data Sets*

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Minimum Necessary**
Policy Number:	**PO-10.1**

Policy Statement

In accordance with federal regulations [45 CFR 164.502(b) and 45 CFR 164.514(d)], the University of Louisville must ensure it applies the minimum necessary standard as appropriate to its uses and disclosures of Protected Health Information (PHI). Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (HCC) shall use and disclose PHI as set forth below.

Procedure

Each college, school, department, and administrative business unit within the HCC will be responsible for identifying, within their area, the following:

A. Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and
B. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Reasonable efforts will be made to limit the access of such persons or classes to only the PHI which is required to carry out their duties.

When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, PHI will be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

An entire medical record may not be used, disclosed, or requested, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

NOTE: The minimum necessary requirement does not apply to:

- Disclosures to, or requests by, a health care provider for treatment;
- Uses or disclosures made to the Individual;
- Uses or disclosures made pursuant to an authorization;
- Disclosures made to the Secretary;

- Uses or disclosures that are required by law and the use or disclosure complies with and is limited to the relevant requirements of such law;
- Uses or disclosures that are required for compliance with applicable requirements of the privacy regulations.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Verification Requirements**
Policy Number:	**PO-10.2**

Policy Statement

In accordance with federal regulations [45 CFR 164.510(b) and 45 CFR 164.514(h)], the University of Louisville must establish guidelines for verifying the identity and authority of Individuals requesting protected health information (PHI).

Procedure

Workforce members shall contact the University Privacy Officer with any questions regarding verification of identity prior to making any Disclosure of PHI.

Disclosures to Family Member, Personal Representative, or Person Responsible for Care of a Patient Regarding an Individual's Location, General Condition, or Death

Verification of identity **is not required** if, upon the exercise of professional judgment, a workforce member discloses information regarding an Individual's location, general condition, or death to the Individual's family member, personal representative, or another person responsible for the care of the patient.

In addition, the verification requirement is considered met in the case of a disclosure to avert a serious threat to health or safety if a workforce member acts on a good faith belief in making the disclosure.

Disclosures to Family Members, Relatives, and Friends When Individual Is Present

When disclosing PHI to a patient's family member, other relative, close personal friend, or any other person identified by the patient as being involved with the patient's care or payment of care:

- Ask the patient if they agree to the disclosure of information to the person and give the patient the opportunity to object to the disclosure.
- If the patient does not object, disclose the information; no verification is needed.

Disclosures to Family Members, Relatives, and Friends When Individual Is Not Present

If an Individual, family member, or friend contacts a Workforce member on behalf of an Individual/patient (for instance, to verify or make an appointment, discuss a billing question, or ask questions about treatment), Workforce members should make a reasonable effort to verify such person is involved in the patient care by asking for identifying information of the patient (i.e., patient's address and zip code; patient's phone number; patient's date of birth). If the Individual can answer these questions and there is nothing in the patient's record indicating any restrictions to disclose the information, the workforce member may choose, in the exercise of professional judgment, to disclose only the specific PHI requested (Minimum Necessary rule applies). (See Privacy Office Policy Number PO-10.1 *Minimum Necessary* for further information).

Conditions on Disclosures

If a disclosure is conditioned on documentation, statements, or representations from the person requesting the PHI, a workforce member may reasonably rely that the documentation, statements, or representations meet the applicable requirements.

For Individuals who have a Power of Attorney, Guardian, or Executor/Executrix, a copy of the paperwork which establishes that relationship should be obtained and placed into the Individual's medical record.

The verification requirements are met if the workforce member relies on the exercise of professional judgment in making a use or disclosure, or acts on a good faith belief in making a disclosure in order to avert a serious threat to health or safety.

Disclosures to Public Officials

Identity of Public Officials

When the disclosure of PHI is to a public official or a person acting on behalf of the public official, a workforce member may rely on any of the following to verify identity:

- *If the request is made in person*: presentation of an agency identification badge, other official credentials, or other proof of government status;
- *If the request is in writing*: the request is on the appropriate government letterhead; or
- *If the disclosure is to a person acting on behalf of a public official*: a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

Authority of Public Officials

When the disclosure of PHI is to a public official or a person acting on behalf of the public official, a workforce member may rely on any of the following to verify authority:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

- Warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.

Note: For guidance regarding disclosures in response to law enforcement, see Privacy Office HIPAA Policy Manual PO-10.7 *Uses and Disclosures without Authorization*.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Treatment, Payment, and Health Care Operations**
Policy Number:	**PO-10.3**

Policy Statement

In accordance with federal regulations [45 CFR 164.506)], the University of Louisville (UofL) has established guidelines for the use or disclosure of protected health information (PHI) for treatment, payment, or health care operations purposes.

Procedure

Except with respect to uses or disclosures of psychotherapy notes, for marketing, or for sale of PHI that require an authorization (see Privacy Office HIPAA Policy PO-10.4 *Authorizations*, PO-22 *PHI for Marketing*, and PO-21 *Prohibition on Sale of Protected Health Information*), or the prohibited uses and disclosures of genetic information for underwriting purposes, the Health Care Component of the University of Louisville Hybrid Covered Entity (HCC) may use or disclose PHI for treatment, payment, or health care operations as set forth below.

- The UofL HCC may use or disclose PHI for its own treatment, payment, or health care operations.
- The UofL HCC may disclose PHI for treatment activities of a health care provider.
- The UofL HCC may disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information.

The UofL HCC may disclose PHI to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the Individual who is the subject of the PHI being requested, the PHI pertains to the relationship, and the disclosure is: 1) For select purposes related to health care operations; or 2) For the purpose of health care fraud and abuse detection or compliance.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Authorizations**
Policy Number:	**PO-10.4**

Policy Statement

In accordance with federal regulations [45 CFR 164.508], the University of Louisville has established guidelines for Individuals to use to request their Protected Health Information (PHI) be disclosed to another person or entity for purposes requiring an Authorization under HIPAA.

Procedure

Questions regarding the use of Authorizations should be directed to the University Privacy Officer. Authorization Forms are available on the Privacy Office website at http://louisville.edu/privacy.

Use of an Authorization

With certain exceptions, an Authorization must be signed before an Individual's PHI can be used for:

- Marketing
- Employment-related purposes
- Purposes not related to Treatment, Payment, and Health Care Operations
- Research
- Schools
- Insurance companies (for enrollment purposes)
- Persons or entities not involved in Treatment, Payment or Health Care Operations.

Copy to the Individual

If UofL seeks an authorization from an Individual for a use or disclosure of PHI, UofL must provide the Individual with a copy of the signed authorization.

Invalid Authorizations

An Individual's PHI may not be used, disclosed or released if an Authorization is invalid. The Privacy Office recommends use of the Authorization forms available on the Privacy Office website to ensure that all required elements are included.

An Authorization is invalid if it contains one of the following defects:

- It does not contain all of the required elements (Contact the Privacy Office with questions regarding the required elements).
- The Authorization has not been filled out completely (one or more required elements are missing).
- It combines a request for general medical information with a request for Psychotherapy Notes.
- The expiration date has passed or the expiration event is known to have occurred.
- The Authorization is known to have been revoked.
- Any material information in the Authorization is known to be false.

Revocation of Authorization

Under the HIPAA Privacy Rule, an Individual has a right to revoke (cancel) an Authorization that he/she submitted to UofL for the use or disclosure of PHI. An Individual's revocation of an Authorization must be in writing.

If an Individual revokes his/her Authorization, UofL must comply with the Individual's request. An Individual's revocation of an Authorization affects only the use and disclosure of

PHI after the date that UofL receives written notice from the Individual.

A Revocation of Authorization Form is available on the University Privacy Office website at http://louisville.edu/privacy)

The Revocation of Authorization form should be filed in the Individual's medical record.

Responding to Requests to Release Protected Health Information (PHI) to an Individual or Third Party

An Individual who requests a copy of his/her medical record may **not** be asked to fill out an authorization; however, UofL may request that the Individual make the request in writing. The Privacy Rule permits an Individual to request a copy of his/her medical record be sent to himself/herself **or** that it be sent to someone else that the Individual designates. For more information regarding an Individual's right to access of his/her medical record, see Privacy Office HIPAA Policy PO-20, *Individual Rights*.

Questions about whether an Authorization is required for the use or disclosure of the Individual's PHI should be directed to the University Privacy Officer or his/her designee.

Individuals may complete an Authorization in person, or send the Authorization to UofL via mail, fax, or email. Authorizations may also be received as an attachment to a third party's request for release of information.

If an Authorization is determined to be defective, the Individual or third party requestor should be contacted to inform them of UofL's inability to complete the release of information. Workforce members should document the reason for the defective Authorization and may attempt to assist an Individual in completing a valid Authorization.

When responding to a request for PHI, include only the PHI that is necessary to meet the Individual's request.

The original request for information and a copy of the requested PHI should be placed in the Individual's medical record.

Prohibition on Conditioning of Authorizations

The University may not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an Authorization, except:

- Research-related treatment may require an Authorization for use and disclosure of PHI for such research (See Privacy Office HIPAA Policy PO-10.8 *Use & Disclosure of PHI – Research* for further information regarding Research Authorizations);
- A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an Authorization requested by the health plan prior to an Individual's enrollment in the health plan in specific circumstances;
- The University may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an Authorization for the disclosure of the PHI to the third party.

Research Authorizations

Refer to Privacy Office Policy PO-10.8 regarding authorizations for research activities.

Refer to University of Louisville Policy HPR-2.01 regarding action(s) required when a required research authorization is not obtained.

Forms

All forms listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Authorization for the Use and/or Disclosure of Protected Health Information
- Revocation of Authorization for the Use and/or Disclosure of Protected Health Information
- Authorization – Media Release
- Authorization – Media Release for UofL Health
- Authorization For Use/Disclosure Of Photographs and Other Imaging For Educational Purposes
- Appointment of Personal Representative/Individuals Involved In Care To Receive Protected Health Information

Related Information

University Privacy Office website: http://louisville.edu/privacy

University of Louisville Policy & Procedure library: https://sharepoint.louisville.edu/sites/policies/library/Pages/Welcome.aspx

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Authorization Required for Patient Imaging for Educational/Instructional Purposes**
Policy Number:	**PO-10.5**

Policy Statement

In accordance with federal regulations [45 CFR §164.508], the University of Louisville (UofL) shall comply with the Privacy Rule by obtaining an HIPAA-compliant Authorization from Individuals prior to taking photographs, video or other imaging of patients taken for educational or instructional purposes.

Procedure

UofL recognizes that photographs, video, x-rays, and other imaging taken of Individuals as part of, or during the course of, treatment qualify as Protected Health Information (PHI) and any Use or Disclosure of PHI is subject to the Privacy and Security Rules. In addition, students at UofL may be required as part of their training and clinical work to obtain imaging for use by UofL faculty for educational or instructional purposes. Such imaging may be subject to use within UofL to educate faculty, residents and students in UofL educational programs.

UofL also recognizes that photographs, video, x-rays, and other imaging taken of Individuals as part of, or during the course of, treatment that qualify as PHI may be desired to be used by UofL faculty for scientific purposes and opportunities available to faculty outside of UofL, including but not limited to, boards/licensure, seminars, presentations, articles, visiting professorships, case reports, and/or professional publications.

Therefore, to the extent imaging is needed for educational and instructional purposes, a University workforce member shall obtain an Authorization from the Individual prior to conducting such imaging. (Authorization form is available on the University Privacy Office website at http://louisville.edu/privacy).

The storage, transmission and security of such imaging shall be subject to the same policies and procedures applicable to all ePHI created, received, transmitted or maintained by the University.

Workforce members are prohibited from taking photos of patients or PHI with personal phones or other electronic devices.

Prior to taking photographs, video, or other imaging, inform the Individual what imaging is being obtained and that the purpose is for educational and/or instructional purposes.

Provide the Individual with the appropriate Authorization form and ask that he/she complete the form.

Instruct the Individual that he/she may revoke the Authorization at any time, provided that the revocation is in writing, except to the extent that UofL has taken action in reliance upon the Authorization (i.e., the imaging has already be used for educational and instructional purposes).

The original Authorization shall be placed in the Individual's medical record.

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Authorization for Use/Disclosure of Protected Health Information for Educational Purposes

Related Information

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Personal Representatives**
Policy Number:	**PO-10.6**

Policy Statement

In accordance with federal regulations [45 CFR §164.502(g)], the University of Louisville (UofL) shall establish guidelines for disclosures of Protected Health Information (PHI) to personal representatives.

Procedure

The Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) shall treat a personal representative as the Individual with respect to PHI, except for unemancipated minors (see below) and for situations of abuse, neglect, or endangerment.

The UofL HCC shall recognize a person as a personal representative if, under applicable law, the person has authority to act on behalf of:

a. A deceased Individual or of the Individual's estate
b. An Individual who is an adult or an emancipated minor for making decisions related to health care.

Personal Representatives: Verification and Authority

The UofL HCC shall confirm the identity and authority of Individuals who present themselves as personal representatives of an Individual if the identity or authority of the personal representative is not already known.

The following must be recognized as personal representatives:

- *If the Individual is an Adult or Emancipated Minor* – The personal representative is a person with legal authority to make health care decisions on behalf of the Individual (for example, a health care Power of Attorney, court appointed legal guardian, general Power of Attorney or durable Power of Attorney that includes the power to make health care decisions). **Exception**: See abuse, neglect, and endangerment situations discussed below.

- *If the Individual is an Unemancipated Minor*- The personal representative is a parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of the minor child. **Exceptions**: As described below in the Unemancipated Minors section or the Abuse, Neglect, and Endangerment situations discussed below.

- *If the Individual is Deceased* – The personal representative is a person with legal authority to act on behalf of the decedent or the estate (for example, Executor or administrator of the estate, or next of kin or other family member).

Unemancipated Minors

If under applicable law, a parent or legal guardian has the authority to act on behalf of an unemancipated minor in making decisions related to health care, then UofL must consider the parent or legal guardian as the personal representative of the unemancipated minor.

Exceptions:

- When the minor is the one who consents to care and the consent of the parent or guardian is not required under State or other applicable law

- When the minor obtains care at the direction of a court or a person appointed by the court

- When and to the extent that the parent or guardian agrees that the minor and the health care provider may have a confidential relationship

Abuse, Neglect, and Endangerment Situations

When a workforce member reasonably believes that an Individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, **or** that treating a person as an Individual's personal representative could endanger the Individual, UofL may choose not to treat that person as the Individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the Individual. (Example: if a physician reasonably believes that providing the personal representative of an incompetent elderly Individual with access to the Individual's health information would endanger that Individual, the physician may decline to provide such access).

Related Information

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Uses and Disclosures Without Authorization**
Policy Number:	**PO-10.7**

Policy Statement

In accordance with federal regulations [45 CFR §164.502(f) & 45 CFR §164.512(a-l)], the University of Louisville (UofL) may use or disclose Protected Health Information (PHI) without written Authorization of the Individual and without giving the Individual an opportunity to object when UofL is permitted or required to do so by state or federal law.

Procedure

Questions regarding the use or disclosure of an Individual's PHI shall be directed to the University's Privacy Officer.

Pursuant to state and federal law, PHI may be used or disclosed for the following purposes:

Uses and Disclosures for a Public Health Activity

(Examples of *public health activities* include disease reports required by state law, vital statistics such as birth and death records, reports of child abuse and neglect, public health surveillance and investigations, reports required by the Food and Drug Administration (FDA), and reports required by the Occupational Safety and Health Administration (OSHA)).

UofL may use or disclose PHI for public health activities and purposes to:

1. A public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to:

    a. The reporting of disease, injury, vital events such as birth or death,

    b. The reporting of the conduct of public health surveillance, public health investigations, and public health interventions; or

    c. At the direction of a Public Health Authority, to an official of a foreign government agency that is acting in collaboration with a Public Health Authority

2. A Public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

3. A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

    a. collection or reporting of adverse events, product defects or problems, or biological product deviations;

    b. to track FDA-regulated products;

    c. to enable product recalls, repairs, or replacement or lookback; or

    d. to conduct post-marketing surveillance.

4. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the University is authorized by law to notify such person, as necessary in the conduct of a public health intervention or investigation.

NOTE: Kentucky State Law requires reporting on such things as disease reporting [KRS 214.010, 902 KAR 2:020], cancer registry [KRS 214.556], TB [KRS 215.590], and public health investigations [KRS 211.220].

NOTE: Per KRS 311.282 UofL may disclose a patient's HIV status to a patient's spouse/ sexual partner, if he/she chooses, but only under certain circumstances.

Abuse, Neglect, Domestic Violence

In the event that a workforce member is suspicious that an Individual is a victim of abuse, neglect, or domestic violence, the Workforce member will contact his/her supervisor or instructor or the University Privacy Officer. [Note: This requirement does not absolve a workforce member from the mandatory reporting obligation required by KRS 620.030 and 209.030].

PHI may be disclosed about an Individual whom the workforce member reasonably believes to be a victim of abuse, neglect, or domestic violence under the following circumstances:

1. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

    - State law **requires** reporting of child dependency, neglect, abuse, or human trafficking and of adult abuse, neglect, or exploitation

    - May only report the following information as required under KY law

- Child Abuse [KRS 620.030]: names and addresses of the child and his/her parents/guardians; child's age; nature and extent of the child's alleged dependency, neglect, or abuse, including any previous charges of dependency, neglect, or abuse, to this child or his or her siblings; name and address of the person allegedly responsible for the abuse or neglect; and any other information that the person making the report believes may be helpful

- Adult Abuse [KRS 209.030]: name and address of the adult or of any other person responsible for his/her care; age of the adult; nature and extent of the abuse, neglect, or exploitation, including any evidence of previous abuse, neglect, or exploitation; the identity of the perpetrator, if known; the identity of the complainant, if possible; and any other information that the person believes might be helpful in establishing the cause of abuse, neglect, or exploitation.

2. If the Individual agrees to the disclosure; **or**

3. To the extent the disclosure is expressly authorized by statute or regulation, **and:**

    - The workforce member, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the Individual or other potential victims (if the workforce member has questions, the workforce member should consult with the workforce member's supervisor or instructor, or the University Privacy Officer); **or**

    - If the Individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI is not intended to be used against the Individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the Individual is able to agree to the disclosure.

In the event that a disclosure described in this section is made, the workforce member, or the workforce member's supervisor or instructor must promptly inform the Individual that such a report has been or will be made, **except if**:

- The workforce member, supervisor or instructor, in the exercise of professional judgment, believes informing the Individual would place the Individual at risk of serious harm; or

- The workforce member, supervisor or instructor would be informing a personal representative, and reasonably believes the personal representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interest of the Individual as determined by UofL, in the exercise of professional judgment.

A copy of the written report, and any accompanying documentation, such as the reasons

why the Individual did not agree to the disclosure or why the personal representative was not informed, is to be placed in the Individual's medical record and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Health Oversight Activities

(Examples of Health Oversight Activities include activities required by law such as audits, surveys, investigations, inspections, licensure, and disciplinary actions necessary for the appropriate oversight of health care systems, government benefit programs, and health care providers subject to certain government regulations).

UofL may disclose PHI for health oversight activities as authorized by laws relating to the health care system, health care provider licensure (including professional Boards), government benefit programs, and regulatory compliance, **except** for information requests related to an investigation of other activity in which the Individual is the subject of the investigation or activity and such investigation or activity does not arise out of, and is not directly related to,:

- the receipt of health care, a claim for public benefits related to health care; or
- qualification for, or receipt of, public benefits or services when an Individual's health is integral to the claim for benefits or services.

A copy of the request and PHI that was used or disclosed is to be placed in the Individual's medical record and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Judicial/Administrative Hearings

(Examples of Judicial/Administrative Hearings include subpoenas, discovery requests, court orders or other lawful process, subject to certain safeguards)

All judicial and administrative requests must be handled by the University Privacy Officer or the Office of University Counsel.

For **court orders** requesting disclosure of an Individual's PHI, the University Privacy Officer will reply to the order, after consulting with the Office of University Counsel, by providing only the PHI expressly authorized by the order.

For subpoenas, discovery requests or other lawful processes **not accompanied by a court or administrative tribunal order**, the University Privacy Officer will reply, after consulting with the Office of University Counsel, by providing only the PHI expressly sought by the subpoena, discovery request or other lawful process **only if the following conditions are met**:

a. the requesting party has provided satisfactory assurances (as defined below) that reasonable efforts have been made to ensure that the Individual who is the subject of the PHI has been given notice of the request; **or**

b. the requesting party provides information that reasonable efforts have been made to secure a qualified protective order satisfying the requirements set forth below.

Satisfactory assurances from the requesting party shall be provided to the University in a written statement and accompanying documentation that:

a. The party requesting such information has made a good faith attempt to provide written notice to the Individual (or, if the Individual's location is unknown, to mail a notice to the Individual's last known address);

b. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the Individual to raise an objection to the court or administrative tribunal; and

c. The time for the Individual to raise objections to the court or administrative tribunal has elapsed, and:

    1) No objections were filed; **or**
    2) The court or the administrative tribunal has resolved all objections filed by the Individual and the disclosure being sought is consistent with such resolution.

A Qualified Protective Order means an order of a court of an administrative tribunal or stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and, at the end of the litigation or proceeding, requires the return of the information to UofL or destruction (including of all copies made) of the information.

A copy of the court order, subpoena, discovery request, qualified protective order or documentation of satisfactory assurances, and the response is to be placed in the Individual's medical record and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

Law Enforcement Purposes

Physical Harm as a Result of an Offense of Violence

UofL may report gunshot, stab wounds or other cases of serious physical harm which he/she reasonably believes to result from an offense of violence as required by State law.

Court Order, Court-Ordered Warrant, Subpoena or Summons Issued by a Judicial Officer or a Grand Jury Subpoena

All court orders, court-ordered warrants, subpoenas or summons issued by a judicial officer, or grand jury subpoenas must be immediately forwarded to the University Privacy Office or the Office of University Counsel. The University Privacy Office or Office of University Counsel will respond to the request or direct the college, school, department, or administrative business unit as to how to respond to the request.

The University Privacy Office or Office of University Counsel will direct the college, school, department, or administrative business unit regarding what documentation should be placed in the Individual's medical record and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

[Note: Some records within the healthcare component may be subject to FERPA requirements].

Administrative Request (Administrative Subpoena, Summons Or Similar Investigative Demand)

All administrative requests must be immediately forwarded to the University Privacy Office or the Office of University Counsel. The University Privacy Office or Office of University Counsel will respond to the request or direct the college, school, department, or administrative business unit as to how to respond to the request.

The University Privacy Office or Office of University Counsel will direct the college, school, department, or administrative business unit regarding what documentation should be placed in the Individual's medical record and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

[Note: Some records within the healthcare component may be subject to FERPA requirements].

To Aid In The Identification Or Location Of A Person Who Is A Suspect, Missing, A Fugitive, Or A Material Witness

If UofL receives a request from a Law Enforcement Official for PHI to aid in the identification or location of a person who is a suspect, missing person, fugitive, or a material witness, the University may disclose **only** the following information:

a. Name and address;

b. Date and place of birth;

c. Social security number;

d. ABO blood type and Rh factor;

e. Type of injury;

f. Date and time of treatment;

g. Date and time of death, if applicable; and

h. A description of distinguishing physical characteristics, such as height, weight, gender, race, hair/eye color, presence or absence of facial hair, scars and tattoos.

UofL **may not** disclose any PHI relating to an Individual's DNA or DNA analysis, dental records, or any typing, analysis or samples of body fluids or tissues.

Any request by a Law Enforcement Official for an Individual's PHI is to be documented in the Individual's medical record. A copy of the written request should be placed in the record, along with appropriate documentation of the University's response and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

Individual Suspected of Being or Is a Victim of a Crime

UofL may disclose PHI in response to a Law Enforcement Official's request for information about an Individual who is, or is suspected to be, the victim of a crime, if the disclosure is not subject to other rules in this section, and if:

(1) The Individual agrees to the disclosure; or

(2) The Individual is unable to agree to the disclosure because of incapacity or other emergency circumstance, **and**:

a. The Law Enforcement Official states that the information is needed to determine whether another person violated the law, and that the information will not be used against the victim;

b. Immediate law enforcement activity depends upon the disclosure of the information, and the activity would be adversely and materially affected by waiting for the Individual to be able to agree; and

c. UofL determines, in the exercise of professional judgment, that disclosure is in the best interests of the victim/Individual.

A copy of the request and PHI disclosed is to be placed in the Individual's medical record. If a paper copy is not available, appropriate documentation should be placed in the Individual's medical record including the date, recipient of the disclosure and description of the information disclosed, and documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

PHI Related to an Individual's Death

UofL may disclose PHI related to an Individual's death to a Law Enforcement Official for the purpose of alerting Law Enforcement Officials about the death if there is a suspicion that the death may have resulted from criminal conduct.

The report to Law Enforcement Officials is to be documented in the Individual's medical record. Include the name and title of the Law Enforcement Official, a description of the information disclosed, the date, time of the report, and the person reporting the death and

documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

Crime on University Premises

Any workforce member who becomes aware of a crime that takes place at the University should immediately report the incident to the University of Louisville Police Department.

If a crime takes place at UofL, the workforce member may disclose PHI to a Law Enforcement Official if a good faith belief exists that the PHI is evidence of the crime. The workforce member must notify the University Privacy Office or University Office of Counsel to report the disclosure as soon as practical after the disclosure.

The disclosure is to be documented in the Individual's medical record and on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*)

Decedents

(Examples of disclosures regarding decedents includes disclosures to medical examiners, coroners or funeral directors to identify a deceased person, determine causes of death, or to carry out funeral related duties).

Coroner or Medical Examiner

UofL may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other purpose required by law.

In the event that a coroner or medical examiner makes a request for PHI, the Workforce member will verify the identity of the agency requesting the information by verifying the request is on official agency letterhead. (See the Privacy Office HIPAA Policy PO-10.2 *Verification Requirements*).

The disclosure is to be documented in the Individual's medical record and on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Funeral Director

UofL may disclose PHI to a funeral director, in a manner consistent with State law, as necessary for the funeral director to carry out his/her duties. This PHI may be disclosed prior to, and in reasonable anticipation of, an Individual's death.

In the event that a funeral director makes a request for PHI, the Workforce member will verify the identity of the funeral home requesting the information, including the name and title of the Individual requesting the information, a description of the information requested, and the date, time of the request. (See the Privacy Office HIPAA Policy PO-10.2 *Verification Requirements*).

The report to a funeral director should be documented in the Individual's medical record, including the name and title of the recipient, a description of the information disclosed, the

date, time of the report, and the person reporting the death. This information should be documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Organ Donation

(Examples of disclosures for organ donation include disclosures for organ, tissue and eye procurement, banking and transplantation).

UofL may disclose a deceased Individual's PHI to an organ procurement organization, or related entities, for purposes of transplantation, donation and banking of cadaveric organs, eyes and tissues.

Any disclosure to an organ procurement organization will be documented in the patient's medical record. Include the name and title of the organization, a description of the information disclosed, the date, time of the report, and the person reporting. This information should be documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Serious Threat to Health & Safety

UofL may disclose an Individual's PHI if the Workforce member believes, in good faith, that use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is made to a person(s) reasonably able to prevent or lessen the threat, including the target of the threat.

a. In the event that a Workforce member obtains information that may avert a threat if disclosed to authorities, the workforce member will immediately notify his/her supervisor or academic instructor, and the University of Louisville Police Department, and the University Privacy Officer or the Office of University Counsel.

b. The Workforce member's supervisor or academic instructor, with guidance from the University Privacy Officer and/or the Office of University Counsel, will determine the validity of the report and if deemed valid, will document the incident and report the necessary information to the appropriate authority.

UofL may disclose an Individual's PHI if necessary for law enforcement authorities to identify or apprehend an Individual if:

a. The Individual admitted his/her participation in a violent crime that is reasonably believed to have caused serious physical harm to another person, **except** if the PHI is learned by UofL in the course of treatment to affect the propensity to commit such criminal conduct or in the course of counseling or therapy (or through a request by the Individual to initiate or to be referred for such treatment, counseling, or therapy);

   or

b. If, based upon all circumstances, it appears that the Individual has escaped from a correctional institution or from lawful custody.

Any disclosure made to law enforcement authorities must include **only** the Individual's statement of admission and the PHI that may be disclosed for law enforcement purposes. (See above for information regarding disclosures to Law Enforcement).

Any disclosure under this section to avert a serious threat to health or safety must be made **in good faith** and **based upon the Workforce member's actual knowledge or reliance on a credible representation** by a person with apparent knowledge or authority.

Document the disclosure in the patient's medical record. Include name of the person reporting, recipient of the information, description of the information reported, date and time. This information must be documented on the Accounting of Disclosures Log. (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Specialized Government Functions

(Examples of disclosures to Specialized Government Functions include Military and veterans' activities, national security and intelligence, medical suitability determinations required by the U.S. Secretary of State, correctional institutions and custodial activities).

UofL may use or disclose an Individual's PHI for the following specialized government functions. Before use or disclosure of any PHI occurs, the Workforce member must notify his/her supervisor or academic instructor, **and** consult with the University Privacy Officer and/or the Office of University Counsel.

In the event that one of the below-referenced military/government agencies makes a request for PHI, the Workforce member will verify the identity of the agency requesting the information by verifying the request is on official agency letterhead. (See the Privacy Office HIPAA Policy PO-10.2 *Verification Requirements*).

Military and veterans' affairs: UofL may disclose PHI of Individuals who are Armed Forces personnel and foreign military personal as requested for activities deemed necessary by military command authorities if notice is published in the Federal Register stating the purpose of the disclosure.

National security and intelligence: UofL may disclose an Individual's PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities. Disclosures made under this section are not required to be included in the Accounting of Disclosures Log.

Protective services for the President and others: UofL may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. §3056 or to foreign heads of state or other persons authorized by 22 U.S.C. §2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. § 871 and 879 (including threats against current and former Presidents and their families).

Medical suitability determinations: UofL may disclose an Individual's PHI to make medical suitability determinations for security clearances, protective service for federal officials, and Foreign Service members and their families.

Correctional Institutions:

Before use or disclosure of any PHI occurs, the Workforce member must notify his/her supervisor or academic instructor, **and** consult with the University Privacy Officer and/or the Office of University Counsel.

UofL may disclose PHI about an Individual or inmate to Law Enforcement Officials or Correctional Institutions as necessary for:

a. The provision of health care to the Individual or inmate;

b. The health and safety of the Individual or other inmates;

c. The health and safety of the officers, employees or others at a Correctional Institution;

d. The health and safety of persons responsible for transport of the Individual or inmate;

e. Law enforcement activities on the premises of the Correctional Institution; or

f. The administration and maintenance of the safety, security, and good order of the Correctional Institution.

The University **may not** disclose PHI for the purposes listed above if the Individual is no longer an inmate and is released on parole, supervised release or otherwise is not in lawful custody.

Disclosures made under this section are not required to be included in the Accounting of Disclosures Log.

Workers' Compensation Benefits

No use or disclosure of PHI shall be made without the Workforce member first notifying his/her supervisor or academic instructor, **and** after consultation with the University Privacy Officer and/or the University's Legal Counsel.

UofL may disclose an Individual's PHI for workers' compensation as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, as authorized by law, which provide benefits for work-related injuries and illness without regard to fault.

A copy of the request and PHI disclosed is to be placed in the Individual's medical record, including date of disclosure, person who made the disclosure, person receiving the PHI, and description of the PHI disclosed. The disclosure should be documented on the Accounting of Disclosures Log (For further information regarding the Accounting of Disclosure Log, see PO-20 *Individual Rights*).

Related Information

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Uses & Disclosures of Protected Health Information - Research**
Policy Number:	**PO-10.8**

Policy Statement

In accordance with federal regulations [45 CFR §164.508, 45 CFR §164.512, 45 CFR §164.514, and 21 CFR 50.25], the University of Louisville (UofL) will comply with the Privacy Rule and the Common Rule governing the use and disclosure of Individual Protected Health Information (PHI) for research purposes.

Investigators are required to maintain and protect the privacy and confidentiality of all personally identifiable information of all human subjects participating in research, except as required by law or released with the written permission of the participant. Individuals who conduct research under the direction of the University of Louisville must develop a plan for each protocol submitted to protect the privacy and confidentiality of participants.

Participants have the right to be protected against invasion of their privacy, to expect that their personal dignity will be maintained, and to expect that the confidentiality of private information will be preserved. The conditions for maintaining confidentiality of the subjects and the research records are required for the life of the data.

The University of Louisville IRB(s) serves as the University's Privacy Board(s).

Procedure

The University of Louisville has and follows written policies and procedures setting forth the ethical standards and practices of the Human Research Protection Program (See University of Louisville Policy Number RES-4.01, *Human Subjects Protection Program Policy Manual)*. The Human Subject Protection Program Policy Manual may be found at http://louisville.edu/research/humansubjects/policies.

Research Authorization

PHI from a covered entity may be used or disclosed for research purposes with a written valid Authorization from the research participant. UofL must ensure that the PHI used or disclosed is done so in accordance with the terms of the Authorization. The requirements for

a Research Authorization are the same as those for a general authorization (see Privacy Office HIPAA Policy PO-10.4 *Authorizations*), with the following special provisions:

1. Unlike other Authorizations, an Authorization for research purposes may state that the Authorization does not expire, that there is no expiration date or event, or that the Authorization continues until all activities related to the study are completed.

2. An Authorization for research purposes may be combined with any other type of written permission for the same or another research study. If the Authorization is for a use or disclosure of psychotherapy notes, it may only be combined with another authorization for a use or disclosure of psychotherapy notes.

Note: Some research studies are designed with blinded or placebo treatment options, which require an Individual to temporarily waive his or her right to access part of the PHI related to the type of treatment assigned. The Research Authorization will indicate whether or not the Individual has agreed to waive this right.

If a research participant revokes his or her Research Authorization, UofL may no longer use or disclose the participant's PHI for research purposes.

A copy of the Authorization must be provided to the participant.

A copy of all Authorizations and any corresponding revocations must be maintained with the research documentation.

Waiver of Authorization Criteria

For a use or disclosure of PHI to a researcher via a Waiver of Authorization, documentation of approval of an alteration or waiver from an IRB/Privacy Board must be in place **prior to** the use or disclosure. The documentation must include **all** of the following:

1. A statement identifying the IRB/Privacy Board and the date on which the alteration or waiver of Authorization was approved; and

2. A statement that the IRB/Privacy Board has determined that the alteration or waiver of Authorization, in whole or in part, satisfies the following criteria:

    a. The use or disclosure of PHI involves no more than minimal risk to the Individuals, based on, at least, the presence of the following elements:

        i. An adequate plan to protect the identifiers from improper use and disclosure;
        ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
        iii. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as require by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the Privacy Rule;

b. The research could not practicably be conducted without the waiver or alteration; and

c. The research could not practicably be conducted without access to, and use of, the PHI.

3. A brief description of the PHI for which use or access has been determined to be necessary by the IRB/PB must be documented;

4. A statement that the waiver of Authorization has been reviewed and approved under either normal or expedited review procedures, and that the IRB/PB followed the requirements of the Privacy Rule and/or the Common Rule.

5. The chair or other member, as designated by the chair, of the IRB/PB must sign the documentation of the alteration or waiver of Authorization.

Action When a Required HIPAA Authorization in Human Subjects Research is not Obtained (University Policy Number HPR-2.01)

When it is discovered that a required HIPAA Authorization is either missing or is incomplete (for instance, without a date or signature), the researcher shall submit a deviation to the IRB/PB. The submission shall include a Corrective Action Plan that includes steps to be taken to prevent future occurrences and sanctions against the Individual responsible.

In addition, the submission shall describe either the plan to obtain a valid Authorization from the subject(s), or to sequester the data.

The IRB/PB, in consultation with the University Privacy Officer, will determine the outcome of the request. No further PHI for the subject(s) shall be obtained or used by the researcher until a final IRB/PB decision is made.

If the IRB/PB determines that the data cannot be maintained for the study, the researcher will not be allowed to use or disclose any PHI from or about the study subject(s). All such PHI shall be eliminated from the active research files and sequestered as appropriate, and an attestation that the required actions have been completed shall be sent to the IRB/PB.

Request for Use/Disclosure for Purposes Preparatory to Research

A researcher may access Individual PHI from a covered entity for purposes preparatory to research as long as the covered entity obtains the following representations from the researcher:

a) Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

b) No PHI will be removed from the covered entity's premises by the researcher in the course of the review; and

c) The PHI for which use or access is sought is necessary for the research purpose (i.e., to design a research study or to assess the feasibility of conducting a study).

The researcher shall limit his/her access to PHI based upon the Minimum Necessary Standard and the Privacy and Security Rules.

Request for Use/Disclosure to Decedents' PHI for Research Purposes

A researcher may access decedents' PHI from a covered entity for research purposes if the covered entity obtains the following representations from the researcher:

a) The use or disclosure being sought is solely for research on the PHI of decedents;

b) The PHI being sought is necessary for the research; and

c) Upon request of the covered entity, documentation of the death of the Individuals about whom PHI is being sought.

The researcher shall limit his/her access to PHI based upon the Minimum Necessary Standard and the Privacy and Security Rules.

De-Identified Information

De-identified information is health information that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual.

Two methods of de-identification are permitted under 45 CFR §165.514(b)-(c):

1. Expert Method. A person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not Individually identifiable determines that the risk is very small that the information could be used alone or in combination with other reasonable available information by an anticipated recipient to identify a subject and documents the methods and results of the analysis that justify the determination. (For further guidance on compliance with the Expert Method, refer to OCR's "Guidance Regarding Methods for De-Identification of Protected Information in Accordance with the HIPAA Privacy Rule" (Nov. 12, 2012), available at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html).

2. Safe Harbor Method. This method requires that the following data elements identifying the Individual (or relatives, employers, or household members of the Individual) be removed, and that the covered entity does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify the Individual:

    a. Names (including initials);
    b. Geographic subdivisions smaller than a state (except the initial three digits of a zip code if the division contains more than 20,000 people);
    c. All elements of dates except year (and for ages greater than 89, unless grouped together into a single category of age 90 or older);
    d. Telephone numbers;
    e. Facsimile numbers;

f. Email addresses;
g. Social Security Numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
l. Vehicle identification and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web addresses – Universal Resource Locators (URLs);
o. Internet Protocol (IP) address numbers;
p. Biometric identifiers, including fingerprints and voiceprints;
q. Full face photographic and any comparable images; and
r. Any other unique identifying number characteristic or code, except a reidentification code (For example: a barcode embedded in an electronic health record or electronic prescribing system if that barcode is unique to a patient or service event; a unique or rare occupation that serves as an identifying characteristic such as the President of the United States).

Information derived from any of the listed identifiers, or parts of the listed identifiers, are not permitted under the Safe Harbor Method. (For example: patient initials or the last four digits of Social Security Numbers.

Re-identification

Re-identification is a process involving the assignment of a unique code to the de-identified data set to permit later re-identification.

A Covered Entity may assign a code or other means of record identification to allow de-identified information to be re-identified by the Covered Entity, provided that: (1) the code or other means of record identification is not derived from or related to information about the Individual and is not otherwise capable of being translated so as to identify the Individual; and (2) the Covered Entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

If a Covered Entity or Business Associate successfully re-identified the subject of de-identified information it maintained, the health information now related to a specific Individual would again be protected by the Privacy Rule and would meet the definition of PHI. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is also considered a disclosure of PHI.

Limited Data Sets

A researcher may use or disclose a Limited Data Set under the following circumstances when a Data Use Agreement is entered into with the recipient of the information:

1. Research
2. Public health studies (For example: use by a private disease registry or public health agency for studies in the private or public sector)
3. Health Care Operations.

A *Limited Data Set* is PHI from which the following direct identifiers of the Individual or of relatives, employers or household members of the Individual have been removed:

1. Name;
2. Postal address, information (information that is allowed: town/city, state and 5-digit 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 identifiers and serial numbers;
13. Web addresses – Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including fingerprints and voiceprints; and
16. Full face photographic images and any other comparable images.

A *Data Use Agreement* (DUA) must include the following minimum terms and conditions:

1. Establish the permitted uses and disclosures of such information by the recipient, which must be for purposes of research, public health, or health care operations. The DUA must not authorize the recipient to use or further disclose the information in a manner that would violate the requirements of the Privacy Rule, if done by the Covered Entity.

2. Establish who is permitted to use or receive the Limited Data Set, **and**

3. Provide that the Limited Data Set recipient will:

    a. Not use the information in a matter inconsistent with the DUA or other laws;
    b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for in the DUA;
    c. Report any use or disclosure of the information that is in violation of the DUA to UofL;
    d. Ensure that any other parties, including subcontractors, that it provides the information to agree to the same conditions as the Limited Data Set recipient in the DUA; and
    e. Not identify the information or contact the Individuals.

UofL is not in compliance with the requirements of the Privacy Rule if UofL knew of a pattern of activity or practice of the Limited Data Set recipient that constituted a material breach or violation of the Data Use Agreement, unless UofL took reasonable steps to cure the breach or end the violation, as applicable; and, if such steps were unsuccessful, discontinued disclosure of the information to the recipient and reported the problem to the Secretary.

A DUA template is available on the University's Privacy Office website at http://louisville.edu/privacy.

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Data Use Agreement

Related Information

Human Subjects Protection Program Office Policy Manual: http://louisville.edu/research/humansubjects/policies

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Safeguards for Storage, Transmission, and Disposal of Protected Health Information**
Policy Number:	**PO-11**

Policy Statement

In accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C), it is the policy of the University of Louisville (UofL) to implement appropriate administrative, technical, and physical safeguards to protect the privacy, security, and integrity of the Protected Health Information (PHI) it maintains. Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) shall adhere to the following safeguards for storage, transmission, and disposal of PHI.

Procedure

Workforce members of the UofL HCC must follow UofL's *Information Security Policies and Standards* (https://louisville.edu/security/policies/policies-standards-list) and this *Privacy Office HIPAA Policy Manual.*

Violations of UofL's *Information Security Policies and Standards* or *Privacy Office HIPAA Policy Manual* may result in disciplinary action up to and including termination of employment. (See Privacy Office Policy PO-14 *Sanctions* for more information regarding sanctions for violations of policies and procedures).

Examples of appropriate safeguards include (but are not limited to) the following:

Storage

- Paper PHI must be stored in areas that are not accessible to Individuals outside of UofL. Preferred location is in a locked room or filing cabinet with access restricted only to authorized Individuals.

- Electronic PHI must be stored on systems and devices (i.e., laptop, phone, flash drive, external hard drive, etc) that are encrypted and protected according to UofL's Information Security Policies and Standards (see link above).

Texting of PHI

- Workforce members **may not** text PHI unless the texted PHI is sent via a UofL-approved text platform for secure texting.

Printers and Copiers

- Appropriate safeguards must be taken to protect PHI contained in printers, copiers, and other devices that can store PHI on internal hard drives. Workforce members should promptly retrieve PHI from printers or other devices to reduce the possibility that it could be accessed or acquired by an unauthorized Individual.

- Printers and copiers which are used for printing or copying PHI should be placed in a location where Individuals who do not have a valid reason to see the information can view the documents or be set up so that UofL credentials are required to access the printed information.

Facsimile Transmissions

- Before sending a fax, workforce members should verify the accuracy of the fax number to be used. Pre-programmed fax numbers are preferred for frequently used fax numbers; however, the fax numbers should be reviewed on a regular basis to ensure they are still accurate.

- A cover page should be included for all fax transmissions. PHI is not to be included on the cover page. All cover pages should include the following confidentiality statement:

    - *CONFIDENTIALITY NOTICE: The information contained in this facsimile message may be privileged and confidential, containing protected health information which is protected by federal privacy regulations (e.g., HIPAA), and is only for the use of the Individual or entity named on this cover sheet. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, the reader is hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If this communication has been received in error, the reader must notify the sender at XXX-XXX-XXXX to arrange for return or destruction of the information received.*

- Fax machines should be placed in a location where Individuals who do not have a valid reason to see the information can access the machine or view received documents or be set up so that UofL credentials are required to access the printed information.

Email Transmissions

- Before sending an email, workforce members should verify the email address of the recipient and ensure that unintended recipients are not included.

- Before sending an email, ensure that attachments are the correct documents.

- Emails which include PHI must be sent in a secure manner in accordance with UofL's Information Security Policies and Standards (see link above).

- Both HIPAA and University policy require that email containing patient/sensitive information be sent securely (encrypted). This is accomplished by using the University's email encryption solution or other University approved processes. If a patient is unable to access encrypted messages and/or **if the patient requests** information be sent unencrypted, the UofL HCC is permitted to send PHI to the Individual via unencrypted email *only after* the workforce member advises the Individual of the risk of the unencrypted email being read by a third party. If the Individual continues to request the information be sent via unencrypted email after being informed of the risk, the Individual's request should be documented on the *HIPAA Unencrypted Email Consent* form (available on the Privacy Office website at http://louisville.edu/privacy) and filed in the Individual's medical record.

Traveling with PHI

- In the event that a workforce member must remove PHI from UofL, the workforce member must ensure that the PHI is appropriately attended and protected from unauthorized access, use, or disclosure, and is returned to UofL as soon as it is no longer needed outside of UofL.

- PHI left inside an unattended vehicle must be placed in the trunk, or, if the vehicle does not have a trunk, the vehicle should be locked with the PHI placed on the floorboard in a manner so as not to be viewed from outside the vehicle (for instance, paper PHI contained in an envelope, on the rear floorboard and tucked under the seat if possible).

- PHI should be taken into the workforce member's home overnight and not left in the vehicle.

- PHI must not be left in an area of the workforce member's home where it may be viewed or accessed by family members or other unauthorized Individuals.

Other Safeguards

Other safeguards include (but are not limited to):

- Restrict the view of computer monitors/screens so that only authorized personnel can see them.

- Conduct telephone or in-person conversations in settings with reasonable safeguards designed to protect the privacy rights of the Individual who is the subject of the information being discussed.

- Limit information left on voice messages to the minimum necessary.

- Call an Individual by first name only from the waiting area.
- Keep filing cabinets closed and/or locked when not in use.
- When mailing PHI, use a trackable method when possible (such as FedEX, UPS, or USPS delivery confirmation).
- Limit information mailed in letters or postcards to the minimum necessary.
- Escort patients or visitors through hallways.
- Use sign-in sheets with the minimum necessary information (e.g., names but not reasons for visit).
- Restrict view of x-ray light boards, procedure scheduling boards, etc., to areas not generally accessible by the public.
- Place medical charts in door hangers so that identifiable information cannot be seen by passersby.

Disposal

- Appropriate safeguards must be followed to protect the privacy of PHI in connection with the disposal of PHI. Depending on the circumstances, proper disposal methods may include (but are not limited to):
    - Shredding or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
    - Maintaining PHI for disposal in a secure area (i.e., restricted access) and using a disposal vendor as a business associate (see Privacy Office HIPAA Policy PO-8 *Business Associate Agreements* for more information about Business Associates) to collect and shred or otherwise destroy the PHI.
    - For PHI on electronic media, disposing based on the guidelines in the Information Security policies.
- Workforce members who use PHI off-site must return all PHI to UofL for appropriate disposal.

For questions regarding proper disposal of PHI, contact the University Privacy Office or the Information Security Office.

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- HIPAA Unencrypted Email Consent

Related Information

University Privacy Office information website: http://louisville.edu/privacy

University Information Security Office website: http://louisville.edu/security

The ISO Policies and Standards are available at http://louisville.edu/security/policies. Per ISO Policy and Standard ISO-001, each member of the campus community is responsible for the security and protection of information resources over which he or she has control, including networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Social Media**
Policy Number:	**PO-12**

Policy Statement

In accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C), it is the policy of the University of Louisville (UofL) to implement appropriate safeguards to protect the privacy, security, and integrity of the Protected Health Information (PHI) it maintains. Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (HCC) shall not post PHI on any form of social and/or digital media.

Procedure

UofL HCC workforce members shall adhere to the University of Louisville Digital Media Policy (OCM-1.04).

UofL HCC workforce members may not post PHI on any social media sites (including, but not limited to, Facebook, Twitter, YouTube, Instagram, LinkedIn, Snapchat, TikTok, WordPress).

UofL HCC workforce members may not upload patient images or patient information on any social media site. The only exception to this prohibition is when the workforce member is uploading/posting the image or information as a part of the workforce member's job responsibilities **and** the information is posted as a part of an approved UofL marketing or communications plan **and** a valid authorization has been executed by the patient for use of the patient's information on social media.

The UofL Office of Communications and Marketing Policy OCM-1.04 permits colleges, schools, departments, and administrative business units within the UofL HCC to have a UofL website or social media site. However, UofL Policy OCM-1.04 and the Privacy Office recommend that UofL websites and social media sites not permit friends, followers, or the general public to create new posts or make comments on the site. However, if UofL HCC websites and social media sites permit the public to create new posts or make comments, the following applies:

- Content shall be monitored to ensure that content that does not meet UofL standards as outlined in UofL Policy OCM-1.04 is not posted. Content that violates HIPAA regulations will be deleted.

- In the event that an Individual, patient, or member of the public posts a comment which includes health information and references services provided by UofL on a public site upon which UofL cannot edit or delete the comment (i.e., Yelp, WordPress, etc), the UofL HCC should request guidance from the Privacy Office before posting a response to the post or comment.
- The UofL HCC website or social media site shall include language on the website that instructs Individuals and patients not to provide or discuss patient information or personal information on the site. The language should include information for patients as to how to contact the Privacy Office, the University Integrity & Compliance Office, or the University of Louisville Compliance Hotline if they have privacy concerns.

If an Individual or patient contacts a UofL HCC workforce member via the workforce member's personal social media site(s), the workforce member shall communicate (off-line) to the Individual/patient that the workforce member is not permitted to correspond via social media. Workforce members shall not post any PHI in his/her response to the Individual or patient.

UofL HCC workforce members are encouraged not to "friend" patients on social media sites or provide patients with the workforce member's personal social media address, email address, or personal phone number.

Related Information

University of Louisville Policy Library:
https://sharepoint.louisville.edu/sites/policies/library/Pages/Welcome.aspx

OCM website: http://louisville.edu/ocm/

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Access to Medical Records of Workforce Member or Workforce Family Member**
Policy Number:	**PO-13**

Policy Statement

In accordance with the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C), it is the policy of the University of Louisville (UofL) to implement appropriate safeguards to protect the privacy, security, and integrity of the Protected Health Information (PHI) it maintains.

Procedure

Workforce members of the Health Care Component of the University of Louisville Hybrid Covered Entity (HCC) may not access their own medical record or the medical record of a family member or an Individual for which the workforce member is a legally authorized representative. This prohibition includes access to an electronic medical record system, paper medical charts or records, and documents stored electronically on UofL devices, laptops, or computer equipment.

Workforce members who wish to access or copy their own, or a family member for whom the workforce member is a legally authorized representative's, medical record must request access to or a copy of the medical record as outlined in PO-10.4 *Authorizations* or PO-20 *Individual Rights.*

Improper or impermissible access by a workforce member to the medical record of a workforce member, colleague, UofL employee, employee of an affiliated health care company, or other Individual may result in sanctions, up to and including termination of employment. (See Privacy Office HIPAA Policy PO-14 *Sanctions* for further information regarding sanctions for violations of HIPAA policy and procedures).

Related Information

University of Louisville Department of Human Resources website: https://louisville.edu/hr/.

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Sanctions**
Policy Number:	**PO-14**

Policy Statement

In accordance with federal regulations [45 CFR §164.530] and University policies, it is the policy of University of Louisville (UofL) to identify, investigate and sanction violations of the UofL Privacy Office HIPAA Policies and Procedures and to mitigate known harmful effects resulting from all such violations.

Procedure

UofL will apply appropriate sanctions against workforce members who fail to comply with the UofL's HIPAA Privacy Policy, the Privacy Office HIPAA Policy Manual, or with HIPAA Privacy and Security Rule requirements (collectively, the "Privacy Policies").

Workforce members found to have inappropriately accessed or disclosed protected health information (PHI) or electronic PHI (ePHI) may be subject to the tiered sanctions as described below.

If the workforce member is a UofL employee, the college, school, department, or administrative business unit where the workforce member is assigned must collaborate with the Department of Human Resources, the Office of the Provost, and/or the University Privacy Office in applying the sanctions.

If a UofL student violates the Privacy Policies, the appropriate program director or instructor will be notified. The program director or instructor, in consultation with the unit or department and the University Privacy Office, will determine and carry out the appropriate action.

When applying sanctions, the college, school, department, or administrative business unit must consider the nature and severity of the violation and the employment sanction history of the Individual.

In addition, reports may be made to the workforce member's professional board as applicable (e.g., Board of Nursing, Board of Licensure for Occupational Therapists) or to appropriate law enforcement agencies.

Tier 1 Accidental, Unintentional, or Unknowing Violation	**Tier 2** Intentional Violation with No Malice *or* Repeated Previous Violations	**Tier 3** Intentional Violation With Malice *or* Unacceptable Number of Previous Violations
Examples: • Misdirected email or fax • Improperly disposing of PHI • Accidentally mailing PHI to the wrong patient's address • Leaving PHI unattended in a public area • Other minor violations of established policies • Non-compliance with required training	Examples: • Sharing UofL credentials with a coworker to help with patient care • Not storing PHI properly when working remotely • Posting PHI on social media (without malice) • Loss of a personal, unencrypted laptop with PHI • Pattern of committing Tier 1 violations	Examples: • Sharing UofL credentials to allow access for malicious purposes • Accessing patient records to gain info for personal gain • Intentionally altering or destroying data • Use or disclosure of PHI to cause harm to an Individual • Unacceptable pattern of Tier 1 or Tier 2 violations • Tier 1 or 2 violation that is disruptive to the work environment or which is adverse to the interests of UofL. • Tier 1 or 2 violation that contributes to the harm of or the unacceptable risk of harm to Individuals or property.
Recommended Sanction • Conference with supervisor - clarification of expectations • Retraining regarding HIPAA policies and procedures • Verbal warning	**Recommended Sanction** • Tier 1 sanctions • Written warning • Final written warning • Leave with or without pay • Loss of privileges within the covered entity or modified job assignments and responsibilities	**Recommended Sanction** • Tier 1 and Tier 2 sanctions • Termination

Sanctions do not apply to a member of UofL's workforce with respect to actions that are covered by and that meet the conditions of the regulatory provisions for:

A. Whistleblowers

B. Workforce member crime victims
C. Filing complaints with the Secretary
D. Testifying or otherwise participating in an investigation, compliance review, proceeding, or hearing under the General Administrative Requirements of HIPAA
E. Opposing an act or practice made unlawful by the HIPAA regulations, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of the privacy regulations

Sanctions must be consistently applied across all instances of non-compliance, in accordance with University Department of Human Resources and Redbook policies.

Applied sanctions must be documented in written or electronic form as required by University Department of Human Resources and Redbook policies.

Related Information

University of Louisville Department of Human Resources website: https://louisville.edu/hr/.

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**No Retaliation Policy**
Policy Number:	**PO-15**

Policy Statement

In accordance with federal regulations [45 CFR §160.316; 45 CFR §164.530] and University policies, it is the policy of the University of Louisville (UofL) that an Individual will not be retaliated against by any Workforce Member for making a complaint to UofL or submitting a complaint to the Secretary of the Department of Health and Human Services.

Procedure

Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) may not retaliate against any Individual exercising his or her rights under the privacy regulations, including:

A. Filing of a complaint to the Secretary of the Department of Health and Human Services
B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing covered in the regulations
C. Opposing any act or practice made unlawful by the regulations, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy regulations.

UofL HCC workforce members may report any instances of retaliation by contacting one of the following:

- University Integrity & Compliance Office (compliance@louisville.edu or (502) 852-8305)
- Compliance Hotline (1-877-852-1167)
- Compliance Hotline Reporting via https://app.mycompliancereport.com/report.aspx?cid=uol
- UofL Privacy Office (privacy@louisville.edu or (502) 852-3803)

Further, workforce members are subject to the UofL Non-Retaliation Policy (Policy Number ICO-1.01), which is available in UofL's Policy Library (http://louisville.edu/compliance/policies/Non-Retaliation_Policy) and which is incorporated herein.

Related Information

University of Louisville Administrative Policy prohibiting retaliation: http://louisville.edu/compliance/policies/Non-Retaliation_Policy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Mitigation**
Policy Number:	**PO-16**

Policy Statement

In accordance with federal regulations [45 CFR 164.530(f)], the University of Louisville (UofL) must mitigate any known harmful effects produced by a violation of the requirements of the Privacy Rule or the Security Rule.

Procedure

UofL will mitigate any known harmful effect resulting from its or its business associate's use or disclosure of Protected Health Information (PHI) that is in violation of the UofL HIPAA Privacy Policy, UofL Privacy Office HIPAA Policies and Procedures, or the requirements of the Privacy Rule and the Security Rule.

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Documentation**
Policy Number:	**PO-17**

Policy Statement

In accordance with federal regulations [45 CFR 164.530(j)], the University of Louisville (UofL) has established guidelines for maintaining required documentation, in written or electronic form, for privacy functions or actions.

Procedure

UofL will adhere to the following documentation retention guidelines, subject to applicable federal and state regulations.

Maintain for six (6) years from the date of its creation or the date when it last was in effect, whichever is later:

- Contents and provision of general HIPAA and entity-specific HIPAA training
- Current and previous versions of the Notice of Privacy Practices
- Titles and offices of those responsible for processing requests for access, amendments, and disclosures
- Sanctions policy and any sanctions actions undertaken by the covered entity
- Items included in the designated record set
- Breach notification actions, including the investigation, notification analysis, and actions to prevent recurrence
- Requests by Individuals for access to their PHI and actions taken to provide the access

- Requests by Individuals for restrictions on disclosure of their PHI and the covered entity's response to the request, if the covered entity agrees to the restriction
- Requests by Individuals for confidential communications and the covered entity's response to the request
- Disclosures that are to be included in an accounting of disclosures and any accounting reports processed
- Requests by Individuals for amendment of their PHI and the covered entity's response to the request
- Complaints received and the covered entity's response to the complaint
- Authorizations, revocations, and waivers of authorization, including resolutions of conflicts among authorizations

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

For retention guidelines for all other documentation, refer to the University of Louisville Policy and Procedure Library at https://sharepoint.louisville.edu/sites/policies/library/Pages/Welcome.aspx.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Breach Response and Notification**
Policy Number:	**PO-18**

Policy Statement

In accordance with federal regulations [45 CFR §164.400, et seq.], the University of Louisville (UofL) will comply with the provisions included in the Privacy Rule and Security Rule regarding response to a potential breach of unsecured Protected Health Information (PHI) and notifications that may be required in the case of breach.

Procedure

Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) must notify the University Privacy Office or the University Information Security Compliance Office immediately upon discovery of any suspected breach of PHI and cooperate with UofL officials in the investigation and mitigation process. (See the Privacy Office HIPAA Policy PO-9 *Privacy & Security Concerns* for more information regarding UofL HCC workforce members' duty to report a privacy or security concern).

Discovery

A breach is treated as discovered as of the first day on which the breach is known by UofL or its Business Associate, or which would have been known by any person exercising reasonable diligence, other than the person who committed the breach.

Investigation and Notification

Investigation of a potential breach of unsecured PHI will be conducted by the UofL Privacy Office, in conjunction with the Information Security Compliance Office, as applicable, or by a UofL HCC workforce member at the direction of the UofL Privacy Office. UofL HCC workforce members must cooperate with the UofL Privacy Office and UofL Information Security Compliance Office to ensure that all information about the incident is included in the investigation. Cooperation includes assistance with interviewing of witnesses and/or workforce members, access to documentation and/or materials involved in the potential breach, access to the college/school/department/administrative business unit's policies and procedures, and discussion regarding appropriate sanctions for workforce members as applicable.

If the investigation determines that the event is a breach which requires written notification to the affected Individuals, the media, or the Secretary, the UofL Privacy Office and/or the UofL Information Security Compliance Office, or their designee, will provide such notification. If deemed by the UofL Privacy Office or the UofL Information Security Compliance Office to require urgency because of possible imminent misuse of unsecured PHI, the UofL Privacy Office, or its designee, may provide information to Individuals by telephone or other means, as appropriate, in addition to the written notices.

In the event that a potential breach occurs while UofL was serving as a Business Associate of a covered entity, the workforce member who discovered the potential breach must immediately notify the UofL Privacy Office or the UofL Information Security Compliance Office of the breach so that notification requirements of the Business Associate Agreement can be assessed. Notification to the covered entity as defined in the Business Associate Agreement will be provided by the UofL Privacy Office, or its' designee.

Documentation

Each college, school, department, and administrative business unit within the UofL HCC must maintain a log of all disclosures of PHI, including potential and actual breaches. For more information regarding the Accounting of Disclosures Log, refer to UofL Privacy Office HIPAA Policy PO-20 *Accounting of Disclosures*.

Forms

The form listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Confidential Question or Complaint Form

Related Information

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s): January 3, 2023
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Notice of Privacy Practices**
Policy Number:	**PO-19**

Policy Statement

In accordance with federal regulations [45 CFR §164.520 & 45 CFR §164.502(i)], the Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) will provide patients with a Notice of Privacy Practices (NPP) outlining the uses and disclosures of Protected Health Information (PHI) that may be made by UofL HCC, and of the Individual's rights and the UofL HCC's legal duties with respect to PHI.

Procedure

NPP Document

HIPAA regulations require the UofL HCC to provide an NPP that is written in plain language and includes specific elements. With limited exception, all members of the UofL HCC must use the NPP template available on the University Privacy Office website (www.louisville.edu/privacy).

The UofL HCC must promptly revise and re-distribute the NPP when there is a material change to the uses or disclosures, the Individual's rights, UofL's legal duties, or other privacy practices stated in the NPP. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the NPP in which such change is reflected.

NPP Availability

The NPP must be prominently displayed at each patient entry and/or registration area of the UofL HCC. The location of the displayed NPP must be such that it is reasonable to expect that Individuals seeking service will be able to read the NPP.

NPPs must be available for Individuals to request to take with them.

Members of the UofL HCC with websites that provide information about customer services or benefits must prominently post the NPP on the website and make the notice available electronically through the website.

The NPP must be made available in alternative formats for Individuals with disabilities and for those Individuals whose primary language is not English.

Provision of Notice

A copy of the NPP must be provided to:

A. Any Individual upon request.
B. An Individual no later than the date of the first date of service, either in person or in electronic format. In an emergency treatment situation, the NPP must be provided as soon as reasonably practicable.

The NPP may be provided to an Individual by email, if the Individual agrees to electronic notice and such agreement has not been withdrawn. If the email transmission fails, a paper copy of the NPP must be provided to the Individual. The Individual who is the recipient of an electronic NPP may obtain a paper copy of the NPP upon request.

When an NPP is revised, it must be made available upon request or after the effective date of the revision.

Acknowledgment

Workforce members must make a good faith effort to obtain a written acknowledgment of receipt of the NPP. If not obtained, the workforce member must document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.

Documentation

A copy of the issued NPP must be kept in the Individual's medical record, along with either the written acknowledgment of receipt of the NPP or documentation of good faith efforts to obtain the written acknowledgment.

Documentation of the acknowledgements or of good faith efforts to obtain the acknowledgement must be retained for at least six (6) years from the date it was obtained or last recorded.

In the event that revisions to the NPP occur, copies of each NPP version issued must be retained for at least six (6) years following the date it is last in effect.

Organized Health Care Arrangements

In certain circumstances, members of the UofL HCC that participate in an organized health care arrangement (OHCA) may comply with the NPP regulations by use of a Joint NPP. Contact the UofL Privacy Office for requests to use a Joint NPP or with questions regarding OHCA regulations.

Forms

All forms listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Notice of Privacy Practices for Health Care Provider (English)
- Notice of Privacy Practices for Health Care Provider (Spanish)
- Notice of Privacy Practices for Health Plan (English)
- Notice of Privacy Practices for Health Plan (Spanish)
- Acknowledgement of Notice of Privacy Practices

Related Information

University Privacy Office website: www.louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Individual Rights**
Policy Number:	**PO-20**

Policy Statement

In accordance with federal regulations [45 CFR §164.502, 45 CFR §164.522, 45 CFR §164.524, 45 CFR §164.526, 45 CFR §164.526], the University of Louisville (UofL) recognizes a patient's Individual rights regarding their Protected Health Information (PHI) and will carry out its obligations regarding such rights as required or permitted by federal and state law. These rights include the right to request restriction of information, right to request communication by alternate means, right to access, right to amendment, and right to an accounting of disclosures.

Procedure

Members of the Health Care Component of the University of Louisville Hybrid Covered Entity (the HCC) will carry out the UofL HCC's obligations regarding an Individual's rights as outlined below.

Individual's Right to Request Restriction

An Individual, or the Individual's personal representative, may request the UofL HCC to restrict the use and disclosure of his/her PHI related to:

- Treatment, Payment or Health Care Operations
- Disclosures to persons involved in the Individual's care
- Disclosures to notify persons, such as family members, personal representatives, or others responsible for the Individual, about PHI directly relevant to the Individual's care or payment for care
- Disclosures to persons when the Individual is or is not present
- Disclosures for disaster relief purposes

With few exceptions, the UofL HCC is not obligated to agree to a requested restriction. However, the UofL HCC is required to agree to an Individual's request to restrict disclosure of PHI about the Individual to a health plan if the disclosure is for payment or health care operations, is not otherwise required by law, and if the information pertains only to a health care item or service the Individual has paid for out-of-pocket in full.

If the UofL HCC agrees to a restriction requested by an Individual, the UofL HCC is required by law to abide by the restriction, unless the restriction prevents the provision of emergency care to the Individual. In the event of such an emergency situation, the PHI may be disclosed to another health care provider; however, the UofL HCC must request that the health care provider receiving the PHI not further use or disclose the information.

An Individual **may not** restrict his/her PHI from being used or disclosed for:

- Requests by the Secretary of Health and Human Services to investigate or determine compliance with the HIPAA Privacy Rule.
- A facility directory, such as use by a hospital to track Individual locations
- Emergency treatment
- Disclosures that do not require an Authorization, such as the disclosure of PHI to public health authorities for reporting a communicable disease.

Responding to a Request for Restriction

If an Individual asks to restrict the use or disclosure of certain health information or records, provide the Individual with the Request to Restrict Use and Disclosure Form (available on the University's Privacy Office website at http://louisville.edu/privacy). The form must be completed and signed by the Individual or Individual's personal representative.

Requests should be processed (granted or denied) as soon as reasonably practicable. The appropriate workforce member of the college, school, department, or administrative unit should review the record to determine whether the information that the Individual wishes to restrict is allowable under the Privacy Rule or whether the information to be restricted will hinder or interfere with the Individual's treatment or payment for the treatment. The workforce member shall consult with the UofL Privacy Officer and/or Office of University Counsel, when necessary, to make a determination.

If the request is **granted**, the restriction request should be documented in the Individual's medical record in a conspicuous area near the PHI that the Individual has restricted. If the request is **denied**, inform the Individual of the denial by using the *Request for Restriction – Denied* form located on the UofL Privacy Office website.

An Individual may request termination of the restriction in the following ways:

1. The Individual may complete the *Request for Restriction* – Termination form (available on the Privacy Office website).

2. The Individual may orally terminate the restriction. Documentation of the request should be included in the patient's medical record.

3. The Individual may provide the UofL HCC with his/her agreement to terminate a restriction in a document that describes the restriction, states the Individual's intent to terminate, and is signed and dated.

If the UofL HCC wishes to terminate the restriction, the appropriate workforce member will send the Individual a written request to terminate the restriction (use the *Request for Restriction – Notice Terminating* Restriction form available on the Privacy Office website).

All documentation related to a request for restriction shall be maintained in the patient's medical record.

Request for Communication by Alternate Means

An Individual may request the UofL HCC to communicate with him/her by alternative means or at an alternative location. This includes how information is sent, faxed, or telephoned to the Individual (e.g., an Individual can ask the UofL HCC not to call him/her at work or to place mailed information into an envelope instead of on a postcard).

Responding to a Request for Communication via Alternate Means

If an Individual requests that communications be directed to an alternative location or by an alternate means, and the request can be reasonably accommodated, the request must be honored.

For Individuals covered under the UofL employee-provided health plan, UofL must accommodate reasonable requests if the Individual/employee indicates that the disclosure of all or part of the PHI could endanger the Individual/employee. UofL may not question the Individual/employee's statement of endangerment.

If the Individual's request cannot be reasonably accommodated, or if the Individual's request would hinder his/her care and treatment or the UofL HCC's billing and payment for services, the UofL HCC is not required to honor the request.

Requests for communication at an alternative location or by an alternative means should be provided to the UofL HCC via a *Request for Confidential Communications* form (available on the Privacy Office website). The form must be completed and signed by the Individual or the Individual's personal representative.

Upon receipt of the completed form, the appropriate workforce member of the college, school, department, or administrative unit should review the form to determine whether the Individual's request can be reasonably accommodated.

- If the request **can be** reasonably accommodated, notice should be provided to the Individual. The completed and signed *Request for Confidential Communications* form should be placed in the Individual's medical record in the same location as the Individual's contact information.

- If the request **cannot be** reasonably accommodated, notice should be provided to the Individual explaining the reason for the denial of the request using the *Request for Confidential Communications Response* form (available on the Privacy Office website). Attach the response provided to the Individual to the original *Request for Confidential Communications* form and place both in the Individual's medical record.

Individual's Right to Access (Inspection or Copying)

Individuals have the right to review and obtain a copy of their PHI in the HCC's designated record set except that the UofL HCC may deny an Individual's request if that information includes:

- Information compiled in the reasonable anticipation of, or use in, a civil, criminal or administrative proceeding.
- Records subject to the Federal Privacy Act.
- Records that are not part of a Designated Record Set.
- Psychotherapy Notes.
- Records obtained from someone other than a Health Care Provider under a promise of confidentiality (for example, a family member who provided confidential information).
- PHI created or obtained by a covered health care provider in the course of research that includes treatment, while the research is in progress, provided that the Individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and that the Individual was informed that the right of access will be reinstated upon completion of the research.

The UofL HCC may also deny an Individual's request for the following reasons. The Privacy Officer and/or the Office of University Counsel should be notified if any of the following reasons will be provided for denial of the Individual's request, before a denial is sent to the Individual.

- A reasonable determination by a health care provider that access is reasonably likely to endanger the life or physical safety of the Individual or another person.
- The PHI contains references to another person, and the health care provider determines that access is reasonably likely to cause substantial harm to such other person.
- The request for access is made by the Individual's personal representative, and the health care provider determines that the provision of access to such personal representative is reasonably likely to cause substantial harm to the Individual or another person.

Quality assessment and incident reports are not part of the Designated Record Set and must not be made available to Individuals for them to inspect or copy.

An Individual may request that the medical records be sent to themselves or to another Individual or company. All requests for records to be sent to another Individual or company must be made in writing, signed by the Individual, and clearly identify the designated person and where to send the copy of the records. (NOTE: An Individual who requests a copy of his/her medical record is not required to complete an Authorization for the Use and/or Disclosure of Protected Health Information form).

The UofL HCC may charge the following fees for the copies (including supplies and labor) and postage. The fee may not include costs associated with searching for and retrieving the requested information.

- *Requests for paper copy of medical records*: First copy is free. Additional pages may be charged at a cost of up to $1.00 per page.

- *Requests for an electronic copy of PHI maintained electronically*: First copy is free. Additional pages may be charged at a cost of up to $1.00 per page, **OR**, the UofL HCC may charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage).

Responding to a Request for Access (Inspection and/or Copying)

For records to be Inspected by/Provided to the Individual or Individual's Representative:

- Individuals may send a written request or fill out a *Request for Access* form (available on the Privacy Office website). Completed forms may be returned by mail, email, fax, or in person.

- **Requests must be processed (granted or denied) within 30 days from the date of receipt of the request.** If the requested information is not maintained or accessible to the college, school, department, or administrative unit on-site, communication should be sent, in writing and within 30 days of the original written request, to the Individual to inform the Individual of the delay in completing the request and that the action will take place no later than 60 days from the receipt of the request.

- The Individual's medical record should be reviewed to determine what information is part of the Designated Record Set and whether any of the information meets the criteria above to be excluded from the request. If the workforce member making this initial determination has a question, clarification should be sought from the University Privacy Officer or Office of University Counsel.

- Once the records have been approved for release, the workforce member will contact the Individual and arrange for release of the information. In the event of an in-person inspection or pick up of the records, the workforce member shall verify the person's identity before releasing the records. (See Privacy Office Policy PO-10.2 *Verification Requirements*)

- If the Individual inspects the medical record at a UofL office allow him/her to inspect in a location or area that reasonably assures privacy. It is not necessary (but advisable) for a workforce member to be present while the Individual inspects the record. However, confidential documents, computer access, and PHI regarding other patients must not be accessible to the Individual. The Individual also must be instructed that he/she cannot remove any original record or make any changes to the record.

- If the person requesting to inspect the record is the Individual's personal representative, photocopy the person's driver's license or government-issued identification card and make sure that the personal representative documentation matches the information in the patient's medical record. If the person is the Individual's Power of Attorney, Guardian, or Executor/Executrix, a copy of the

authorizing document must be received at the time of, or in advance of, the inspection date.

- All requests to inspect and/or for copies must be documented in the patient medical record including the denial of any such requests and any receipts acknowledging delivery/pickup of the information.

- An Individual may request that medical records be sent to another Individual or organization.

Denial of a Request for Inspection and/or Copying

- If, in consultation with the UofL Privacy Officer or Office of University Counsel, a determination is made that some or all of a request should be denied, the following steps shall be taken:

    - A written denial shall be sent to the Individual, or personal representative, using the *Request for Access – Denied* form available on the Privacy Office website).

    - If the denial is reviewable per the HIPAA Privacy Rule, the Individual, or personal representative, will be informed of his/her right to have the denial reviewed by another licensed health professional who did not participate in the original decision to deny access. The Individual, or personal representative, will be informed that he/she must request review in writing. The reviewing official must determine within a reasonable period of time (no more than 30 days) whether to deny access.

- The Workforce member, in consultation with the UofL Privacy Officer and/or Office of University Counsel, will provide written notice to the Individual, or personal representative of the determination of the designated reviewing official and will, based on the designated reviewing official's determination, either allow or deny the access.

- The request for review of denial and its results will be maintained in the Individual's electronic record for a minimum of six (6) years.

Individual's Right to Amend or Correct

An Individual, or the Individual's personal representative, has the right to amend incorrect, inaccurate, or incomplete PHI contained in his/her record.

An Individual does not have the right to amend all of the PHI contained in his/her record. The UofL HCC may deny an Individual's request if the PHI:

- Was not created by the University of Louisville, unless the Individual provides the University with a reasonable basis to believe that the original source of the PHI is no longer available;
- Is not part of a Designated Record Set;
- Is already accurate and complete;
- Are psychotherapy notes;
- Is compiled in reasonable anticipation of, or for use in, a criminal, civil or administrative proceeding; or

- Was obtained from someone other than a health care provider under a promise of confidentiality.

Responding to a Request to Amend or Correct

- Individuals who wish to amend records may do via a written request or a *Request for Amendment* form (available on the Privacy Office website). The form must provide a reason to support the Individual's requested amendment.

- The Individual's medical record should be reviewed to determine whether any of the information meets the criteria above to be excluded from the request. If the workforce member making this initial determination has a question, clarification should be sought from the University Privacy Officer or Office of University Counsel.

- **A request must be processed (granted or denied) within 60 days from the date of receipt of the completed form.** If a request cannot be processed within 60 days, the UofL HCC may extend the time to reply for an additional 30 days by providing the Individual with a written statement describing the reason(s) for the delay and the date in which the UofL HCC will respond to the request. Only one extension of time is permitted by the Privacy Rule.

- If the request is **granted**, the appropriate workforce member shall:

    - Timely contact the Individual making the request to inform the Individual that his/her request was granted and to ask the Individual to identify the relevant persons, including health care providers, who should receive the amended information. The workforce member should obtain the Individual's agreement to have the UofL HCC inform the identified parties about the amendment. (See the *Request for Amendment – Granted* and *Identification of Persons to be Notified* forms on the Privacy Office website).

    - Make the appropriate amendment to the Individual's PHI. Do not change, obliterate, or delete the existing information in the Individual's record. Append the amendment to the record or provide a link to the location of the amendment in the record.

    - Make reasonable efforts to inform and provide the amended information, within a reasonable time, to (1) parties identified by the Individual, and (2) parties, such as Business Associates, who the UofL HCC knows have the Individual's PHI that is the subject of the amendment and who could foreseeably rely on the un-amended information to the detriment of the Individual.

- If the request is **denied,** the appropriate workforce member shall timely inform the Individual of the denial using the *Request for Amendment – Denied* form available on the Privacy Office website.

- If the Individual sends a written statement of disagreement to the University, the appropriate workforce member, in consultation with the University's Privacy Officer and/or Office of University Counsel, will prepare a written rebuttal which will be mailed to the Individual. The workforce member must identify the PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the Individual's request, the letter of denial, the Individual's written

statement of disagreement, and UofL's rebuttal, if available, to the Designated Record Set. (A *Request for Amendment Statement of Rebuttal* form is available on the Privacy Office website).

- For all future disclosures of the Individual's PHI that is the subject of the amendment:
    - The Individual's written statement of disagreement (if submitted) must be included with all subsequent disclosures of the PHI, or, in the alternative, the UofL HCC may include an accurate summary of the information.
    - If the Individual did not submit a written statement of disagreement, the UofL HCC must include the Individual's request to amend and the denial letter, or, in the alternative, the UofL HCC may include an accurate summary of the information.
    - If a transaction of PHI does not allow the transmission of the additional information concerning the request to amend, the UofL HCC should separately transmit the additional information to the recipient of the transaction.
- The names and titles of the persons responsible for receiving and processing requests to amend must be documented with all Requests for Amendment. Retain all documentation regarding Requests for Amend for at least six (6) years.
- If the UofL HCC receives an amendment of an Individual's PHI from another health care provider or entity, the appropriate workforce member must amend the Individual's PHI as contained in a Designated Record Set in the University's medical record.

Individual's Right to an Accounting of Disclosures

An Individual, or an Individual's personal representative, has the right to request an accounting of the disclosures of his/her PHI made by the HCC during the previous six (6) years.

An Accounting of Disclosures provides an Individual with information regarding:

- The date that PHI was disclosed;
- The name and address (if known) of the entity or person receiving the PHI;
- A brief description of the PHI that was disclosed;
- A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure; or a copy of the written request, if any, to use the PHI as required by the Secretary, Department of Health and Human Services; or a copy of the request for the PHI, if any, for which an Authorization is not required (see Privacy Office Policy PO-10.7 *Uses and Disclosures Without Authorization*);
- The frequency, periodicity or number of disclosures made to the person or entity; and

- The date of the last disclosure occurring in the accounting period if multiple disclosures were made to a single person or entity.

An Accounting of Disclosures does **not** include the following disclosures made by the UofL HCC:

- To carry out Treatment, Payment and Health Care Operations;
- Directly to the Individual or his/her personal representative;
- Incidental disclosures;
- In response to an Authorization;
- To include the Individual in a facility directory;
- To persons involved in the Individual's care or for notification purposes;
- For national security of intelligence purposes;
- As part of a Limited Data Set; and
- To Correctional Institutions or Law Enforcement Officials.

If a Health Oversight Agency or Law Enforcement Official provides the University with a written or oral statement notifying UofL that an Accounting of Disclosures will reasonably impede the agency's or official's activities, UofL must not inform the Individual about these disclosures. The Health Oversight Agency or Law Enforcement Official must provide UofL with a time period after which the information may be disclosed in an accounting requested by the Individual (no longer than 30 days).

Responding to a Request for Accounting of Disclosures

A written request for an Accounting of Disclosures must be signed by the Individual or the Individual's personal representative.

The appropriate workforce member of the college, school, department, or administrative unit should review the form to determine if the requested information may be disclosed to the Individual in an accounting of disclosures. The workforce member should contact the University Privacy Officer or Office of University Counsel with questions.

A request must be processed within 60 days from the date of receipt of the completed form. If the UofL HCC cannot provide an accounting within 60 days, an additional 30 days may be available if the Individual is provided with a written statement describing the reason for the delay and the date by which the UofL HCC will provide the accounting. Only one extension is permitted by the Privacy Rule. **Requests for extensions of time should only be requested after consultation with the University Privacy Office or University Office of Counsel.**

The Accounting of Disclosure should be prepared using the Accounting of Disclosures to an Individual form (available on the University's Privacy Office website.

If this is the first request for an accounting by the Individual in a 12–month period, the Individual must not be charged for any fees incurred by the UofL HCC to prepare the accounting. If an Individual submits a subsequent request for an accounting in the same 12-month period, the Individual should be informed that a charge of $25.00 plus postage will be assessed. The Individual should be provided the opportunity to modify or withdraw the request in order to reduce or avoid any fees.

A copy of the Accounting of Disclosures request and the response to the request should be placed in the Individual's medical record.

If the UofL HCC determines that an Individual's request for an accounting should be denied, the UofL HCC will request a consultation with the University Privacy Office or University Office of Counsel prior to informing the Individual of the denial. A written notice will be provided to the Individual which explains the reason(s) for the denial. This notice shall be filed with the original request in the Individual's medical record.

Disclosure Log

To assist in responding to an Individual's request for an Accounting of Disclosures, the University Privacy Office recommends use of a Disclosure Log in order to keep track of all disclosures of PHI regarding an Individual. The Disclosure Log is available on the University's Privacy Office website.

Forms

All forms listed below may be found on the Privacy Office website at http://louisville.edu/privacy.

- Request for Restriction of Protected Health Information
- Request for Restriction of Protected Health Information Response – Denied
- Termination of Request for Restriction of Protected Health Information
- Notice of Termination of Restriction of Protected Health Information
- Request for Confidential Communications
- Request for Confidential Communications Response
- Request To Access, Inspect & Copy Protected Health Information
- Request To Access, Inspect & Copy Protected Health Information Response - Granted
- Request To Access, Inspect & Copy Protected Health Information Response - Denied
- Request for Amendment of Protected Health Information
- Request for Amendment of Protected Health Information Response - Granted
- Persons to be Notified of Amendment of Protected Health Information
- Request for Amendment of Protected Health Information Response – Denied
- Statement of Disagreement (to Denied Request for Amendment)
- Statement of Rebuttal (to Denied Request for Amendment)
- Accounting of Disclosures Tracking Log
- Request for Accounting of Disclosures
- Request for Accounting of Disclosures Response - Granted
- Request for Accounting of Disclosures Response – Denied

Related Information

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**Prohibition on the Sale of PHI**
Policy Number:	**PO-21**

Policy Statement

In accordance with federal regulations [45 CFR §164.502 & 45 CFR §164.508], the University of Louisville or a Business Associate will not directly or indirectly receive remuneration in exchange for any protected health information (PHI) of an Individual except pursuant to a valid authorization that includes specifics as to the sale/exchange of the PHI or a permitted exception.

Procedure

Workforce members will consult with the University Privacy Officer and/or Office of University Counsel before any use or disclosure for sale of PHI occurs.

Related Information

Federal regulations provide exceptions to this prohibition for remuneration for:

- Public health activities
- Research purposes, subject to limitations (cost of data preparation and transmittal)
- Treatment and Payment purposes (including Disclosure of PHI to a collection agency for purposes of payment collection activities)
- Health Care Operations related to sale, merger or transfer of a Covered Entity
- Business Associates under Business Associate Agreement
- Individuals (to provide a copy of the Individual's PHI)
- Required by Law
- Other situations determined by the Secretary

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

Privacy Office
HIPAA Policy Manual

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**PHI for Marketing**
Policy Number:	**PO-22**

Policy Statement

In accordance with federal regulations [45 CFR §164.508(a)(3)], the University of Louisville (UofL) shall comply with HIPAA regarding the use or disclosure of Protected Health Information (PHI) for marketing purposes.

Procedure

UofL will ensure its disclosures for marketing purposes are made in accordance with the privacy regulations.

Authorizations must be obtained for any use or disclosure of PHI for marketing, except if the communication is in the form of:

A. A face-to-face communication made by UofL to an Individual; or
B. A promotional gift of nominal value provided by UofL.

If the marketing involves financial remuneration to or from UofL from a third party, the authorization must state that such remuneration is involved.

NOTE: HIPAA regulations regarding marketing are complex and additional state and federal laws govern marketing practices and activities conducted by UofL; therefore, questions regarding marketing activities should be directed to the UofL Privacy Office, the University Office of Counsel, and/or the University Office of Communications and Marketing.

Related Information

Examples of Marketing:

- A drug manufacturer receives a list of patients from a covered Healthcare Provider and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patient.

- Communication from a physician or other Covered Entity informing former patients about a cardiac facility, that is not part of the entity, that can provide a baseline EKG for $39, when the communication is not for the purpose of providing treatment advice.

The following examples are NOT Marketing:

- A hospital or physician uses its patient list to announce the arrival of a new specialist or the acquisition of new equipment (e.g., x-ray machine or MRI) through a general mailing or publication.
- A communication is not Marketing if it is made for treatment of the Individual: A primary care physician refers an Individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.
- An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the patient.

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):

University of Louisville
Privacy Office
215 Central Avenue
Suite 205
Louisville, KY 40208
(502) 852-3803
privacy@louisville.edu

Policy Name:	**PHI for Fundraising**
Policy Number:	**PO-23**

Policy Statement

In accordance with federal regulations [45 CFR §164.514(f)], the University of Louisville (UofL) shall comply with HIPAA regarding the use or disclosure of Protected Health Information (PHI) for fundraising purposes.

Procedure

UofL, if raising funds for its own benefit, may disclose certain PHI to a Business Associate or an "institutionally related foundation" without an Authorization, provided that certain conditions are met.

The following types of information may be disclosed:

- Demographic information relating to an Individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an Individual;
- Department of service information;
- Treating dentist/physician;
- Outcome information; and
- Health insurance status.

This information can be disclosed for fundraising purposes **only if** UofL's Notice of Privacy Practices informs Individuals that they may be contacted for fundraising purposes and that they have the right to opt out of such communications (See the *University of Louisville Notice of Privacy Practices* for further information).

With each fundraising communication made to an Individual for fundraising purposes, UofL must provide the Individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an Individual to elect not to receive further fundraising communications may not cause the Individual to incur an undue burden or more than a nominal cost.

If an Individual requests to opt out, UofL, its' Business Associate, and/or any institutionally related foundation shall honor such request. UofL **may not** make further fundraising communications to an Individual after the Individual has elected to opt-out and not to receive further fundraising communications.

UofL may provide an Individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

UofL may not condition treatment or payment on the Individual's choice with respect to the receipt of fundraising communications.

Institutionally related foundation.

In order to qualify as an "institutionally related foundation," a foundation must meet two requirements:

1. Foundation must qualify as a 501(c)(3) nonprofit charitable foundation; and
2. Foundation's charter must include an explicit linkage to UofL.

In the absence of an Individual's Authorization, UofL shall not disclose PHI to foundations that do not qualify as "institutionally related."

NOTE: HIPAA regulations regarding fundraising are complex and additional state and federal laws govern fundraising activities conducted by UofL; therefore, questions regarding fundraising activities should be directed to the UofL Privacy Office, the University Office of Counsel, and/or the University Office of Communications and Marketing.

Related Information

University Privacy Office website: http://louisville.edu/privacy

HIPAA Regulations and Guidance on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html.

Effective Date: December 1, 2020
Revision Date(s):
Reviewed Date(s):