UNIVERSITY OF LOUISVILLE

HIPAA Privacy Guidance

UNIVERSITY OF LOUISVILLE

Table of Contents

DEFINITIONS

UNIVERSITY OF LOUISVILLE

AR-01 TRAINING

AR-02 SHADOWING

AR-03 NOTICE OF PRIVACY PRACTICES

AR-04 BUSINESS ASSOCIATES

AR-05 MINIMUM NECESSARY

UNIVERSITY OF LOUISVILLE

AR-06 VERIFICATION REQUIREMENTS

PURPOSE
GUIDANCE
Conditions on Disclosures
Disclosures to Public Officials

AR-07 SAFEGUARDS FOR STORAGE, TRANSMISSION, AND DISPOSAL OF PHI

PURPOSE
GUIDANCE
Storage
Printers and Copiers
Facsimile Transmissions
Email Transmissions
Confidentiality Statement
Other Safeguards
Disposal

AR-08 BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

PURPOSE
GUIDANCE

AR-09 DESIGNATION OF PRIVACY OFFICIAL

PURPOSE
GUIDANCE

AR-10 SANCTIONS

PURPOSE
GUIDANCE

AR-11 NO RETALIATION POLICY

PURPOSE
GUIDANCE

AR-12 MITIGATION

PURPOSE
GUIDANCE

AR-13 POLICIES AND PROCEDURES

PURPOSE
GUIDANCE
Changes to Policies or Procedures
Changes to Privacy Practices Stated in the Notice of Privacy Practices

AR-14 DOCUMENTATION

PURPOSE
GUIDANCE

AR-15 DESIGNATED RECORD SET

PURPOSE

UNIVERSITY OF LOUISVILLE

UNIVERSITY OF LOUISVILLE

UD-08 VICTIMS OF ABUSE, NEGLECT, OR DOMESTIC VIOLENCE

PURPOSE
GUIDANCE
Other Elements

UD-09 HEALTH OVERSIGHT ACTIVITIES

PURPOSE
GUIDANCE
Other Elements

UD-10 JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

PURPOSE
GUIDANCE
Court Order
Subpoena, Discovery Request, or Other Lawful Process
Qualified Protective Order
Disclosures without Satisfactory Assurance
Other Elements

UD-11 LAW ENFORCEMENT

PURPOSE
GUIDANCE
Required by Law
Limited Information for Identification and Location Purposes
Victims of a Crime
Decedents
Crime on Premises
Reporting Crime in Emergencies
Note: Information may also be disclosed to avert a serious threat or injury. For additional guidance, see UD-14 To Avert a Serious Threat or Injury.
Other Elements

UD-12 DECEDENT INFORMATION

PURPOSE
GUIDANCE
Coroners and Medical Examiners
Funeral Directors
Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes
Family, Friends, and Others involved in the Care of the Individual prior to Death
Uses and Disclosures for Research Purposes
Other Elements

UD-13 RESEARCH

PURPOSE
GUIDANCE
De-identified Data
Limited Data Set
Authorization
Waiver or Alteration of Authorization
Preparatory to Research

UNIVERSITY OF LOUISVILLE

UD-21 PROHIBITION ON SALE OF PROTECTED HEALTH INFORMATION

UNIVERSITY OF LOUISVILLE

Definitions

Following is a list of HIPAA definitions relevant to or used throughout the privacy guidance documents.

Breach

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.

Breach excludes:

A. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the privacy regulations.

B. Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the privacy regulations.

C. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

D. Except as provided above, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the privacy regulations is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

   1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   2. The unauthorized person who used the PHI or to whom the disclosure was made;

   3. Whether the PHI was actually acquired or viewed; and

   4. The extent to which the risk to the PHI has been mitigated.

UNIVERSITY OF LOUISVILLE

Business Associate

A. Except as provided in paragraph D of this definition, business associate means, with respect to a covered entity, a person who:

1. On behalf of the covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of the covered entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA regulations, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

2. Provides, other than in the capacity of a member of the workforce of the covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of PHI from the covered entity or arrangement, or from another business associate of the covered entity or arrangement, to the person.

B. A covered entity may be a business associate of another covered entity.

C. Business Associate includes:

1. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI.

2. A person that offers a personal health record to one or more individuals on behalf of a covered entity.

3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

D. Business Associate does not include:

1. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

2. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR §164.504(f) apply and are met.

3. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

4. A covered entity participating in an organized health care arrangement that performs a function or activity described in paragraph A(1) of this definition for or on behalf of the organized health care arrangement, or that provides a services as described in paragraph A(2) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Correctional Institution

Correctional institution means 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

Covered entity means:

A. A health plan

B. A health care clearinghouse

C. A health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations.

Covered Function

Covered functions means 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

Data aggregation means, 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 the 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

Designated record set means:

A. A group of records maintained by or for a covered entity that is:

   1. The medical records and billing records about individuals maintained by or for a covered health care provider;

   2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

   3. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

B. For purposes of this paragraph, 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

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure

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

Electronic Media

Electronic media means:

A. Electronic storage material on which data are or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

B. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, 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 if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic Protected Health Information

Electronic protected health information means protected health information that is transmitted by or maintained in electronic media.

Employer

Employer means 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

Family member means, 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).

1. First-degree relatives include parents, spouses, siblings, and children.

2. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

3. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

4. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic Information

Genetic information means:

A. Subject to paragraphs B and C of this definition, with respect to an individual, information about:

   1. The individual's genetic tests;

   2. The genetic tests of family members of the individual;

   3. The manifestation of a disease or disorder in family members of such individual; or

   4. 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.

B. Any reference in the HIPAA regulations to genetic information concerning an individual or family member of an individual shall include the genetic information of:

   1. A fetus carried by the individual or family member who is a pregnant woman; and

   2. Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

C. Genetic information excludes information about the sex or age of any individual.

Genetic Services

Genetic services means:

A. A genetic test;

B. Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

C. 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

Health care means 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

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

A. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

B. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from the activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

C. Underwriting (except for the prohibition on the use of genetic information for this purpose), enrollment, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR §164.514(g) are met, if applicable;

D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

E. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

F. Business management and general administrative activities of the entity, including, but not limited to:

1. Management activities relating to implementation of and compliance with the requirements of the HIPAA regulations;

2. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to the policy holder, plan sponsor, or customer.

3. Resolution of internal grievances;

4. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following the activity will become a covered entity and due diligence related to the activity; and

5. Consistent with the applicable requirements of 45 CFR §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health Care Provider

Health care provider means 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

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

A. 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

B. 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

Health oversight agency means 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

Health plan means 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)).

A. Health plan includes the following, singly or in combination:

1. A group health plan
2. A health insurance issuer
3. An HMO
4. Part A or Part B of the Medicare program under title XVIII of the Act
5. The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
6. The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152
7. An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1))
8. An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy
9. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
10. The health care program for uniformed services under title 10 of the United States Code
11. The veterans health care program under 38 U.S.C. chapter 17
12. The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
13. The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

14. An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

15. The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28

16. A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals

17. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2))

B. Health plan excludes:

1. Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

2. A government-funded program (other than one listed in paragraph (A)(1)–(16) of this definition):

   a. Whose principal purpose is other than providing, or paying the cost of, health care; or

   b. Whose principal activity is the direct provision of health care to persons; or the making of grants to fund the direct provision of health care to persons.

Indirect Treatment Relationship

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

A. The health care provider delivers health care to the individual based on the orders of another health care provider; and

B. 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.

UNIVERSITY OF LOUISVILLE

Individually Identifiable Health Information

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

A. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

B. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

C. That identifies the individual; or

D. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate

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

Law Enforcement Official

Law enforcement official means 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:

A. Investigate or conduct an official inquiry into a potential violation of law; or

B. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Manifestation or Manifested

Manifestation or manifested means, 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

A. Except as provided in paragraph B of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

B. Marketing does not include a communication made:

1. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

2. For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

a. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

b. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

c. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

C. Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Organized Health Care Arrangement

Organized health care arrangement means:

A. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

B. An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

   1. Hold themselves out to the public as participating in a joint arrangement; and

   2. Participate in joint activities that include at least one of the following:

      a. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

      b. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

      c. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

C. A group health plan and a health insurance issuer or HMO with respect to the group health plan, but only with respect to protected health information created or received by the health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in 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 paragraph (D) of this definition and health insurance issuers or HMOs with respect to the group health plans, but only with respect to protected health information created or received by the health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of the group health plans.

Payment

Payment means:

A. The activities undertaken by:

1. Except for the prohibition of the use of genetic information for underwriting purposes, a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

2. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

B. The activities relate to the individual to whom health care is provided and include, but are not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

a. Name and address;

b. Date of birth;

c. Social security number;

d. Payment history;

e. Account number; and

f. Name and address of the health care provider and/or health plan.

Protected Health Information

A. Protected health information means 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.

B. 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

Psychotherapy notes means 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

Public health authority means 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

Required by law means 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

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

Sale of Protected Health Information

Sale of protected health information (PHI) means 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:

A. For public health activities (see guidance UD-07 Public Health Activities).

B. For research (see guidance UD-13 Research) 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.

C. For treatment and payment purposes (see guidance UD-02 Treatment, Payment, and Operations).

D. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for the due diligence related to such activity (see definition of Health Care Operations and guidance UD-02 Treatment, Payment, and Operations).

E. 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 (see

guidance AR-04 Business Associates), 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.

F. To provide an individual with a copy of their PHI (see guidance PR-01 Patient Access to Protected Health Information and PR-04 Accounting of Disclosures).

G. When required by law (see guidance UD-06 Required by Law).

H. 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 PHI for such purpose or a fee otherwise expressly permitted by other law.

Secretary

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

Subcontractor

Subcontractor means 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

Treatment means 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

Except as provided below, underwriting purposes means, with respect to a health plan:

A. 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);

B. 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);

C. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

D. 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

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.

Use

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

Workforce

Workforce means 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 the covered entity or business associate, whether or not they are paid by the covered entity or business associate.

AR-01 Training

Purpose

To establish guidelines for training of the covered entity's workforce on the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Guidance

All members of a covered entity's workforce must be trained on the HIPAA Privacy and Security regulations and on the entity-specific policies and procedures with respect to protected health information, as necessary and appropriate for the members of the workforce to carry out their job functions.

Training Requirements

Training shall be provided:

A. To each new member of the covered entity workforce within 30 days after the person joins the workforce.

B. To each member of the workforce whose functions are affected by a material change in the policies or procedures, within 30 days after the material change becomes effective.

General HIPAA Training

The HIPAA Privacy and HIPAA Security training are required for members of the workforce:

A. In any position that would allow direct or indirect contact with personal health or health-related financial information – electronic, paper, verbal, in the lab – for either a clinical or a research purpose; or

B. With direct contact with patients

In addition, if an individual will be performing human subject research that is reviewed by the IRB and that involves access to individually identifiable health information, HIPAA Research (or a research refresher course, as applicable) is required.

Policies and Procedures Specific to the Covered Entity

A. Each covered entity area must train members of its workforce with regard to the covered entity's privacy policies and procedures or protocols, which are required to be maintained in written or electronic format and accessible by members of its workforce.

B. Entity-specific training shall be based upon the workforce member's job or role within the entity.

Consideration of HIPAA Training from Previous Jobs or Experience

HIPAA training of workforce members must be based in the covered entity's own privacy practices and reflect its implementation of the Privacy Regulations. Therefore, a covered entity cannot 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 the workforce for two weeks or less, the training described above is not required. In this case, the covered entity area/unit shall have the individual sign the Confidentiality Agreement available on the University Privacy Office website (http://louisville.edu/privacy/imgs/confidentiality-agreement-word).

The covered entity area/unit shall provide a copy of the signed Confidentiality Agreement to the workforce member, maintain a copy for its own records, and forward a copy to the University Privacy Office.

Enforcement

The responsibility for enforcement of HIPAA training remains at the department level.

Training Documentation

Each covered entity area/unit shall maintain documentation of training related to general training and to entity-specific HIPAA Privacy and Security policies and procedures provided to its workforce. For entity-specific training, such documentation shall include a copy of the content that was delivered as well as:

A. The name of the individual receiving the training;

B. The date the training was provided; and

C. The topic of the content that was delivered.

AR-02 Shadowing

Purpose

To establish guidelines for shadowing activities within the covered entity

Guidance

When an individual (Participant) is not affiliated with the covered entity or otherwise authorized to enter entity's area, a covered entity must ensure that safeguards are in place to protect confidentiality of protected health information (PHI) before allowing the Participant to shadow or observe patient care within the covered entity.

The covered entity shall facilitate the shadowing / observing activities, which includes:

A. Verifying the Participant's identity

B. Determining appropriateness of objectives

C. Assigning a staff or faculty member responsible for oversight

D. Ensuring the Participant's understanding of patient privacy and confidentiality.

The Participant may not actively participate in patient care.

The covered entity shall ensure that the Participant signs the Confidentiality Agreement available on the University Privacy Office website (http://louisville.edu/privacy/imgs/confidentiality-agreement-word). The covered entity shall forward the agreement to the University Privacy Office, maintain a copy in the covered entity, and provide a copy to the Participant.

If the Participant will be shadowing for more than two weeks, then the University's formal HIPAA training is required (see guidance AR-01 Training).

During the shadowing, at the beginning of each patient encounter, the covered entity member responsible for oversight of the Participant must introduce the Participant to the patient, explain why the 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 Participant. The agreement or objection may be obtained in written or verbal form.

The covered entity member responsible for oversight must limit the use and disclosure of PHI to the minimum level necessary to meet the Participant's objectives (see guidance AR-05 Minimum Necessary).

AR-03 Notice of Privacy Practices

Purpose

To establish guidelines for the development and distribution of the Notice of Privacy Practices

Guidance

A covered entity must provide its patients with a Notice of Privacy Practices (NPP) describing how the covered entity may use and disclose protected health information (PHI) of its patients, what privacy rights its patients can expect, and what legal obligations the covered entity has for protecting PHI.

NPP Document

The covered entity shall provide a notice that is written in plain language and that contains the elements required by the regulation (see Attachment AR-03 – NPP Elements). The covered entity shall use the template available on the University Privacy Office website (http://louisville.edu/privacy/templates/templates).

The covered entity shall promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. 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 notice in which such material change is reflected.

Provision of Notice

The covered entity shall provide the notice:

A. To any individual upon request.

B. To an individual no later than the date of the first date of service, either in person or electronic. In an emergency treatment situation, notice shall be provided as soon as reasonably practicable.

C. At the service delivery site, posted in a clear and prominent location where it is reasonable to expect that individuals seeking service will be able to read the notice.

D. On its website, if the website provides information about the covered entity's customer services or benefits. The notice shall be prominently displayed on the website and shall be available electronically.

E. By email, if the individual agrees to electronic notice and the agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice shall be provided to the individual.

Whenever the notice is revised, the covered entity shall make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (C) above, if applicable.

Acknowledgment

The covered entity shall make a good faith effort to obtain a written acknowledgment of receipt of the notice. If not obtained, the covered entity shall document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.

Documentation

The covered entity shall document compliance with the notice requirements by retaining copies of the notices issued, and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain the written acknowledgment.

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

B. In the event that revisions to the NPP occur, copies of each NPP version issued shall be retained indefinitely.

Organized Health Care Arrangements

Covered entities that participate in an organized health care arrangement (OHCA) may comply with this section by a joint notice, provided that:

A. The covered entities participating in the OHCA agree to abide by the terms of the notice with respect to PHI created or received by the covered entity as part of its participation in the OHCA;

B. The joint notice contains the elements required by the regulations (see Attachment AR-03 – NPP Elements), except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

   1. Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

   2. Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

   3. If applicable, states that the covered entities participating in the OHCA will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the OHCA.

C. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement with respect to all others covered by the joint notice.

Attachment AR-03 – NPP Elements

Required Elements

Header. The notice shall contain the following statement as a header or have it otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

Uses and Disclosures. The notice shall contain each of the following elements and shall describe them as enforced by HIPAA or by other applicable law, whichever law is more restrictive.

A. A description of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations, including at least one example for each

B. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the individual's written authorization

C. A statement that the individual's written authorization is required for:

   1. Uses and disclosures of psychotherapy notes (if the entity records or maintains such notes)

   2. Uses and disclosures of PHI for marketing

   3. Disclosures that constitute a sale of PHI

D. A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke the authorization

Separate Statements for Certain Uses or Disclosures. If the covered entity intends to engage in the following activities, the description shall include a separate statement that:

A. The covered entity may contact the individual to provide information about treatment alternatives or other health-related benefits and services

B. The covered entity may contact the individual to raise funds for the covered entity and that the individual has a right to opt out of receiving these communications

Individual Rights. The notice shall contain statements of the individual's rights with respect to PHI and a brief description of how the individual may exercise the right to:

A. Request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction unless the disclosure is to a health insurance plan regarding a service that the individual has paid for out of pocket in full

B. Receive confidential communications of PHI

C. Inspect and copy PHI

D. Amend PHI

E. Receive an accounting of disclosures of PHI

F. Obtain a paper copy of the notice upon request

G. Receive notification in case of a breach

Covered Entity's Duties. The notice shall contain a statement that the covered entity:

A. Is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI

B. Is required to abide by the terms of the notice currently in effect

C. Reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. The statement shall also describe how it will provide individuals with a revised notice.

Complaints. The notice shall contain:

A. A statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated

B. A brief description of how the individual may file a complaint with the covered entity

C. A statement that the individual will not be retaliated against for filing a complaint

Contact. The notice shall contain the name, or title, and telephone number of a person or office to contact for further information.

Effective Date. The notice shall contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

Optional Element

If the covered entity elects to limit the uses or disclosures that it is permitted to make, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or to avert a serious threat to health or safety.

AR-04 Business Associates

Purpose

To establish guidelines for determining the existence of a business associate relationship and for administering Business Associate Agreements when required

Guidance

A covered entity must determine when a business associate relationship exists and must ensure a Business Associate Agreement is executed when required.

The covered entity shall document satisfactory assurances through a Business Associate Agreement (BAA) that meets the applicable requirements in the regulations (see Attachment AR-04.3 - BAA Elements).

If the covered entity knows 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 covered entity shall take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement, if feasible.

If the business associate knows of a pattern of an activity or practice of the subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the contract or other arrangement, the business associate shall take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement, if feasible.

Determining a Business Associate Relationship

When establishing a business relationship for the purpose of providing any type of service to the covered entity, the covered entity shall evaluate whether or not the relationship constitutes a business associate relationship (see Attachments for flowcharts to assist with this process). If it is determined that the service provider is a business associate, a BAA shall be drawn up and executed as part of establishing the business relationship and associated contracts.

In addition, the covered entity shall periodically review its existing business relationships to determine whether or not each constitutes a business associate relationship (see Attachments for flowcharts to assist with this process). If it is determined that such a relationship does exist but a

BAA does not currently exist, the covered entity shall immediately begin work on establishing the agreement.

Establishing the Business Associate Agreement

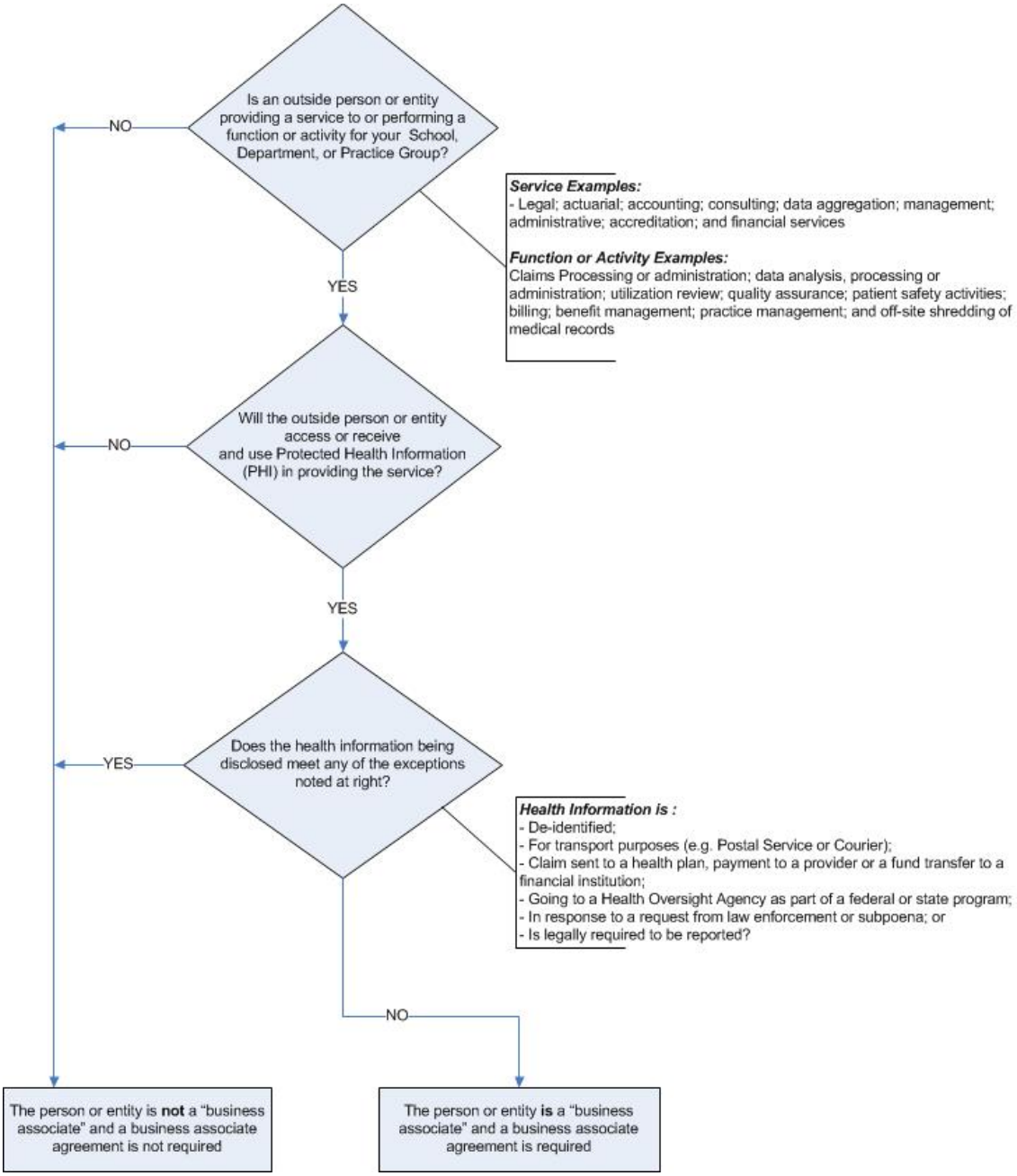
When establishing a BAA, the covered entity shall ensure that the agreement delineates the uses and disclosures of PHI that are permitted and required by the business associate. To do this, the covered entity shall use the BAA template available on the University Privacy Office website (http://louisville.edu/privacy/templates/templates) to ensure that the most current template is being used and that all of the elements required by the regulations are included (see Attachment AR-04.3 - BAA Elements).

If the other party proposes changes to the BAA template or proposes using a template of its own, the covered entity shall send the BAA to the University Privacy Office for review before agreeing to or signing the document.

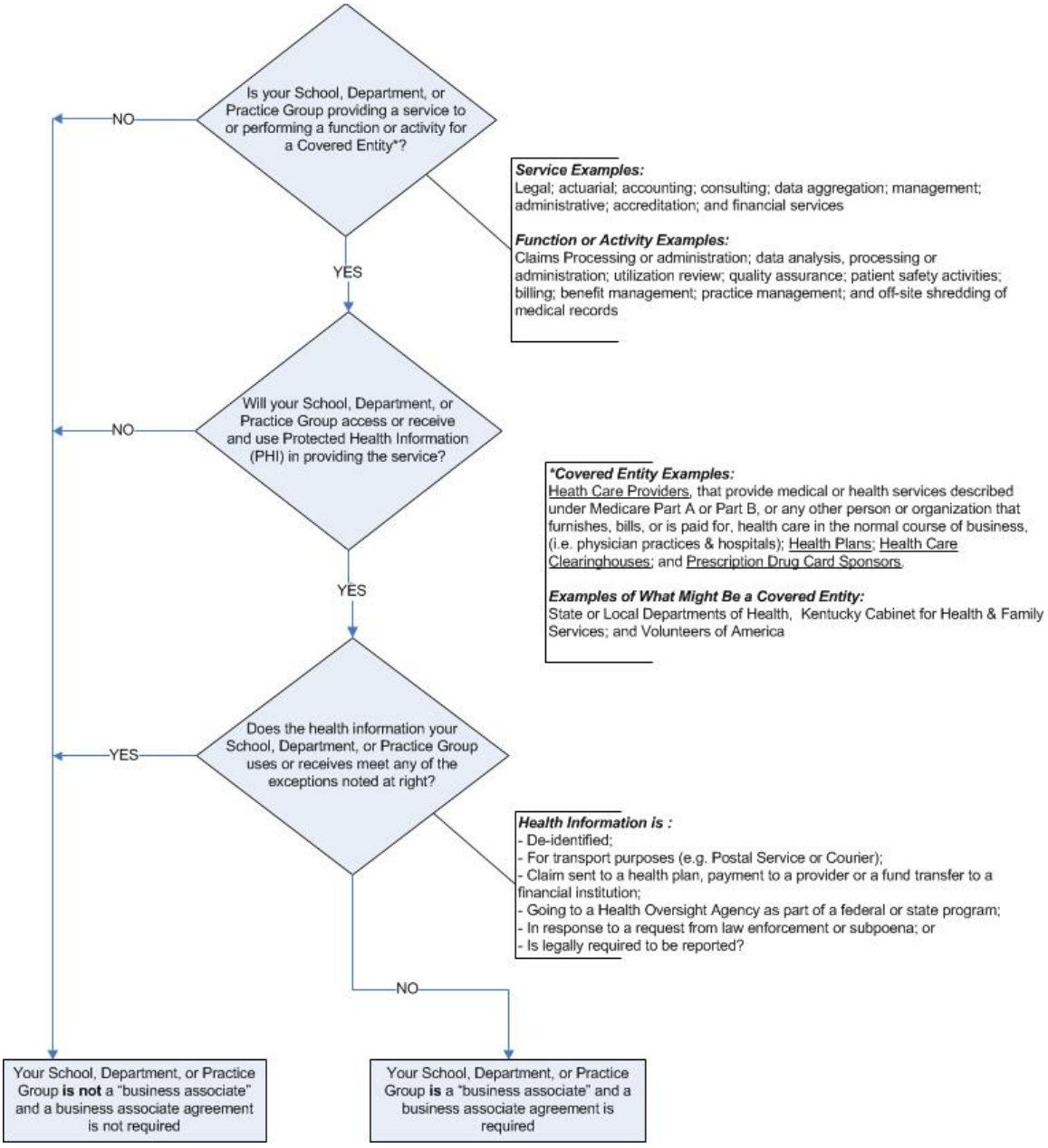
The covered entity shall proceed to get signatures only if the University's template is used or, if changes are made or another template is used, only after the University Privacy Office has approved the document.

Once the agreement is fully executed, the covered entity shall send a copy of the BAA to the University Privacy Office.

Attachment AR-04.1 - BAA Decision Flow Chart for Covered Entities



Attachment AR-04.2 - BAA Decision Flow Chart for Business Associates



Attachment AR-04.3 - BAA Elements

Required Elements

The Business Associate Agreement (BAA) shall provide that the business associate will:

A. Not use or further disclose the information other than as permitted or required by the contract or as required by law

B. Use appropriate safeguards and comply with the Security Rule with respect to electronic PHI, to prevent use or disclosure of the information other than as provided for by its contract

C. Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information. Notice of such a breach shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach. Business associate further agrees to make available in a reasonable time and manner any information needed by covered entity to respond to individuals' inquiries regarding said breach.

D. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information

E. Make available PHI in accordance with 45 CFR §164.524 (access of individuals to PHI)

F. Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 CFR §164.526 (amendment of PHI)

G. Make available the information required to provide an accounting of disclosures in accordance with 45 CFR §164.528 (accounting of disclosures of PHI)

H. To the extent the business associate is to carry out a covered entity's obligation under the HIPAA privacy regulations, comply with the requirements of the regulations that apply to the covered entity in the performance of such obligation.

I. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with the HIPAA regulations

J. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible

K. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate

Optional Elements

The Business Associate Agreement (BAA) may not authorize the business associate to use or further disclose the information in a manner that would violate the regulatory requirements, if done by the covered entity, except that the contract may permit the business associate to use and disclose PHI:

A. For the proper management and administration of the business associate

B. To carry out the legal responsibilities of the business associate

C. To provide data aggregation services relating to the health care operations of the covered entity.

The BAA may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in the preceding paragraph, if:

A. The disclosure is required by law; or

B. The business associate

1. Obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

2. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

If the underlying agreement does not address Kentucky's security and breach notification law, this must be included in the BAA.

Desired Elements

If the BAA is being prepared for a University covered entity, it is preferred that the following elements are included in the BAA:

A. Upon prior written request, make available during normal business hours at business associate's offices all records, books, agreements, policies, and procedures relating to the use and/or disclosure of PHI to the covered entity to determine the business associate's compliance with the terms of the BAA

B. Business associate agrees that any electronic PHI it acquires, maintains, or transmits will be maintained or transmitted in a manner that fits the definition of secure PHI as that term is defined by HIPAA and any subsequent regulations or guidance from the Secretary of the Department of Health and Human Services (DHHS).

C. Business associate agrees to indemnify CE for reasonable cost to notify the individuals whose information was breached, including any costs, damages, attorney fees, fines, identity theft prevention/monitoring costs.

AR-05 Minimum Necessary

Purpose

To establish guidelines for appropriate uses and disclosures of protected health information

Guidance

A covered entity must ensure it applies the minimum necessary standard as appropriate to its uses and disclosures of protected health information (PHI).

Workforce Requirements

The covered entity shall identify:

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.

The covered entity shall make reasonable efforts to limit the access of such persons or classes to PHI consistent with the identified categories. Attachment AR-05.1 HIPAA Role-Based Access may be used to assist with these classifications.

Use and Disclosure Requirements

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, the covered entity or business associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The covered entity shall limit such PHI, to the extent practicable, to the limited data set (see guidance UD-18 Uses and Disclosures of Limited Data Sets) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.

In the case of the disclosure of PHI, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure. Covered entities and business associates may rely on requests from other covered entities and business associates as the minimum necessary.

The covered entity may not use, disclose, or request an entire medical record, 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. The covered entity shall document in its policies and procedures when the use or disclosure of the entire medical record is permitted.

For a disclosure or request that is made on a routine and recurring basis, the covered entity shall implement policies and procedures (which may be standard protocols) that limit the PHI disclosed or requested to the amount reasonably necessary to accomplish the purpose for which the disclosure or request is made. Attachment AR-05.2 Routine Requests and Disclosures may be used to assist with these classifications.

For all other disclosures or requests for PHI, the covered entity shall:

A. Consider whether PHI in the form of a limited data set is sufficient;

B. Develop criteria designed to limit the PHI disclosed or requested to the information reasonably necessary to accomplish the purpose for which disclosure is sought or the request is made; and

C. Review requests for disclosure on an individual basis in accordance with such criteria.

Exceptions

The minimum necessary requirement does not apply to:

A. Disclosures to or requests by a health care provider for treatment

B. Uses or disclosures made to the individual

C. Uses or disclosures made pursuant to an authorization

D. Disclosures made to the Secretary

E. 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

F. Uses or disclosures that are required for compliance with applicable requirements of the privacy regulations

Attachment AR-05.1 HIPAA Role-Based Access

The list below should be used as an example only. Each covered entity should customize the list to include the specific roles in their covered entity and the privileges for each role. "Medical Record" should be changed to list the various types or categories of records available and the privileges for each based on the role.

Role	**Document**	**Privileges***		
		R	**W**	**S**
Business Manager	Billing Record (if relevant for business management activities; otherwise aggregate data only)	X		
	Medical Record (if relevant for business management activities; otherwise aggregate data only)	X		
Coder / Biller	Billing Record	X	X	X
	Medical Record	X		
Communications / Marketing / Public Relations	*Aggregate data only; no access to PHI without patient authorization*			
Compliance Staff	Billing Record	X		
	Medical Record	X		
Human Resources Staff	Billing Record (if relevant for an HR-related investigation; otherwise aggregate data only)	X		
	Medical Record (if relevant for an HR-related investigation; otherwise aggregate data only)	X		
Information Technology Staff	Billing Record (if necessary for IT activities)	X		
	Medical Record (if necessary for IT activities)	X		
Medical Assistant	Medical Record	X	X	X
Medical Records Clerk	Billing Record	X		
	Medical Record	X	X	
Office Assistant	*Depends on specific tasks*			
Office / Practice Manager	Billing Record	X	X	X
	Medical Record	X	X	

Role	Document	Privileges*		
		R	W	S
Physician, Nurse Practitioner, Other Provider	Billing Record	X		
	Medical Record	X	X	X
Receptionist	Schedule	X	X	X
Registered Nurse / Other Nurse	Billing Record	X		
	Medical Record	X	X	X
Scheduler	Schedule	X	X	X
Social Worker	Medical Record	X	X	
* R – Read; W – Write; S – Sign				

Attachment AR-05.2 Routine Requests and Disclosures

The list below should be used as an example only. Each covered entity should customize the list to add any requests for disclosure that are routine for their population and activities.

Requester	Purpose	Disclosure / Response
Attorney	Gather Information for Preparation / Defense of a Lawsuit or Criminal Action	With subpoena and once satisfactory assurances have been received, may disclose those records that have been specifically requested
Collection Agency	Collection of Covered Entity's Past Due Accounts	Information needed for collection (e.g., name, contact information, amount owed)
Coroner	Investigation of Suspicious Death	Information needed to investigate cause of death
Employer	Drug Screening	Drug test results
	Employment Screening	Information relevant to the physical and/or mental requirements of the occupation
Funeral Home	At or in Reasonable Anticipation of Death	Information needed for receipt and preparation of the body
Insurance Company – Health	Claims Processing	Information needed to support claim and substantiate services provided
Insurance Company – Life	Evaluate Individual's Condition for Issuance of Life Insurance Policy	Information needed to evaluate individual's overall condition
Physician / Other Covered Entity	Treatment	Information relevant to the anticipated treatment
Police / Law Enforcement	Criminal Investigation	Information needed for the specific law enforcement purpose
Researcher	Recruitment or Participation in a Clinical Trial	Information mentioned in the Waiver or Research Authorization
	Retrospective Records Review	Information mentioned in the Waiver

Requester	Purpose	Disclosure / Response
School	Immunization Records	Name and immunization history
	Release to Return	Name, date of return, limitations (if any and if relevant to school activities)
	Release for Sports / Other Activities	Name, limitations (if any and if relevant to the activities)
	Records for Treatment to be Provided by School Nurse	Information needed for the specific treatment to be provided
State Data Commission	Statewide Registry	Information needed for the registry
Workers' Compensation	Evaluate a Claim	Information relevant to the specific claim

AR-06 Verification Requirements

Purpose

To establish guidelines for verifying the identity and authority of individuals requesting protected health information

Guidance

A covered entity must develop and implement protocols for verifying the identity and authority of individuals requesting protected health information (PHI).

Prior to any disclosure of PHI, the covered entity shall:

A. Except with respect to disclosures requiring an opportunity for the individual to agree or to object, verify the identity of a person requesting PHI and the authority of any such person to have access to PHI, if the identity or any such authority of such person is not known to the covered entity; and

B. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the disclosure.

Conditions on Disclosures

If a disclosure is conditioned on particular documentation, statements, or representations from the person requesting the PHI, the covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

The verification requirements are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure requiring an opportunity for the individual to agree or to object or acts on a good faith belief in making a disclosure 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, the covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity:

A. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

B. If the request is in writing, the request is on the appropriate government letterhead; or

C. 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, the covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority:

A. 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;

B. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

AR-07 Safeguards for Storage, Transmission, and Disposal of PHI

Purpose

To establish guidelines for implementing safeguards of protected health information

Guidance

A covered entity must implement appropriate administrative, technical, and physical safeguards to protect the privacy, security, and integrity of the protected health information (PHI) it maintains.

The covered entity shall follow the University's Information Security Policies and Standards in providing safeguards for electronic PHI.

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

Storage

The covered entity shall:

A. Store paper PHI in areas that are not accessible to individuals outside the covered entity, preferably in a locked room or filing cabinet with access restricted to authorized individuals

B. Store electronic PHI on systems and devices that are encrypted according to the University's Information Security Policies and Standards

Printers and Copiers

Covered entities shall provide appropriate safeguards to protect PHI contained in printers, copiers, and other devices that can store PHI on internal hard drives. (See the IT website for further information http://louisville.edu/it/departments/itech-xpress-and-printing-copier-management/printing/advantages-of-printing-and-copier-management)

Facsimile Transmissions

The covered entity shall:

A. Verify the accuracy of the phone number to be used

B. Include a cover page that contains a confidentiality statement

C. Place the facsimile machine in a location where individuals outside the covered entity cannot access the machine or see received data

Email Transmissions

If the covered entity permits its workforce members to send PHI via email transmissions, the covered entity shall ensure its workforce members:

A. Verify the email address of the recipient

B. Send email containing PHI in a secure manner in accordance with the University's Information Security Policies and Standards.

If an individual who is the subject of the PHI requests PHI by email, covered entities are permitted to send the PHI through unencrypted emails if they have advised the individual of the risk of the email being read by a third party, and the individual still prefers the unencrypted email.

Confidentiality Statement

All facsimile and email transmissions containing PHI shall be accompanied by 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 shall notify the sender at XXX-XXX-XXXX to arrange for return or destruction of the information received.

Other Safeguards

Other safeguards include (but are not limited to):

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

B. Conducting 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

C. Limiting information left on voice messages to the absolute minimum necessary

D. Limiting information mailed in letters or postcards to the absolute minimum necessary

E. Escorting patients or visitors through hallways

F. Using sign-in sheets with the minimum necessary information (e.g., names but not reasons for visit)

G. Restricting view of x-ray light boards, procedure scheduling boards, etc., to areas not generally accessible by the public

H. Placing medical charts in door hangers so that identifiable information cannot be seen by passersby

I. Ensuring that any PHI that is removed from the covered entity is appropriately attended and protected from unauthorized access, use, or disclosure, and is returned to the covered entity as soon as it is no longer needed outside the covered entity setting

Disposal

The covered entity shall apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI) in connection with the disposal of the information.

In determining an appropriate method of disposal, the covered entity shall assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be

disposed. Depending on the circumstances, proper disposal methods may include (but are not limited to):

A. 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

B. Maintaining PHI for disposal in a secure area (i.e., restricted access) and using a disposal vendor as a business associate (see guidance AR-04 Business Associates) to collect and shred or otherwise destroy the PHI

C. For PHI on electronic media, disposing based on the guidelines in the Information Security policies

Workforce members who use PHI off-site shall return all PHI to the covered entity for appropriate disposal.

AR-08 Business Continuity and Disaster Recovery Plans

Purpose

To establish guidelines for business continuity and disaster recovery plans

Guidance

A covered entity must develop and implement specific plans to ensure it can perform necessary operations in the event of an emergency, including disaster recovery protocols as appropriate for its business operations.

The covered entity shall base its policies and procedures on the University's Information Security policy on Business Continuity and Disaster Recovery.

The covered entity shall document its business continuity and disaster recovery plans in writing and shall maintain and/or distribute the plans in a redundant fashion locally and off-site to ensure at least one copy is available in the event a disaster occurs or electronic access to the plan is not available.

AR-09 Designation of Privacy Official

Purpose

To establish guidelines for the designation of a privacy official and contact person

Guidance

A covered entity must designate a privacy official, liaison, or contact person who is responsible for the development and implementation of the policies and procedures of the covered entity and for receiving privacy complaints and questions.

The covered entity shall document the designations in written or electronic form.

This is the contact information for some of the entities on HSC:

University of Louisville, Privacy Officer
(502)852-3803

University of Louisville Physicians, HIPAA Privacy Officer
(502)588-4520

Catholic Health Initiatives, Corporate Responsibility Officer
University of Louisville Hospital | James Graham Brown Cancer Center
(502)587-4041

AR-10 Sanctions

Purpose

To establish guidelines for sanctions related to non-compliance with HIPAA policies and procedures

Guidance

A covered entity must develop and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or with the HIPAA Privacy and Security Rule requirements.

If the individual is a University employee, the covered entity shall work with the University Human Resources department in applying the sanctions.

When applying sanctions, a covered entity shall consider the nature and severity of the violation and the employment sanction history of the individual. Examples of sanctions may include, but are not limited to:

A. Conference with supervisor - clarification of expectations

B. Retraining in HIPAA and entity-specific policies and procedures

C. Written warning

D. Leave with or without pay

E. Loss of privileges within the covered entity or modified job assignments and responsibilities

F. Termination

G. Government agencies may also impose penalties that may include exclusion from federal programs, civil penalties, and criminal charges

Sanctions do not apply to a member of the covered entity'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

The covered entity shall consistently apply its sanctions across all instances of non-compliance, in accordance with its policy.

The covered entity shall document in written or electronic form the sanctions that are applied.

The covered entity shall ensure that all members of its workforce receive and acknowledge training of its sanctions policy for non-compliance with privacy and security policies and regulations.

AR-11 No Retaliation Policy

Purpose

To establish guidelines for non-retaliation against workforce members for exercising their rights under the privacy regulations

Guidance

A covered entity or business associate must adopt and implement a no-retaliation policy to ensure no retaliatory action is made against any individual exercising his or her rights under the privacy regulations, including:

A. Filing of a complaint to the Secretary

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

The covered entity or business associate shall follow the University's policy on non-retaliation, available in the University's Policy Library (http://louisville.edu/compliance/policies/Non-Retaliation_Policy).

The covered entity or business associate shall report any instances of retaliation by contacting one of the following:

A. Institutional Compliance Office (compliance@louisville.edu; 502-852-8305)

B. Compliance Helpline (1-877-852-1167)

C. "Compliance Helpline Reporting" option on ULink found under the External Links section of the Faculty/Staff tab

AR-12 Mitigation

Purpose

To establish guidelines for mitigating known harmful effects produced by violation of the privacy regulations

Guidance

A covered entity must mitigate any known harmful effect resulting from its or its business associate's use or disclosure of protected health information that is in violation of its policies and procedures or the requirements of the privacy regulations.

AR-13 Policies and Procedures

Purpose

To establish guidelines for implementing policies and procedures in accordance with the privacy regulations

Guidance

A covered entity must implement policies and procedures designed to comply with the standards, implementation specifications, or other requirements of the privacy regulations.

All policies and procedures, and changes to policies and procedures, shall be documented in written or electronic form.

Changes to Policies or Procedures

The covered entity shall change its policies and procedures as necessary and appropriate to comply with changes in the law and in the privacy regulations. Whenever there is a change in law that necessitates a change to the entity's policies or procedures, the covered entity shall promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices (Notice), the covered entity shall promptly make the appropriate revisions to the Notice in accordance with the policy regarding the Notice.

The covered entity may change, at any time, a policy or procedure that does not materially affect the content of the Notice, 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 covered entity shall provide and document training of its workforce members regarding any changes to entity's policies and procedures to the extent such change affects the workforce member's job responsibilities or access, use, or disclosure of PHI.

Changes to Privacy Practices Stated in the Notice of Privacy Practices

When the covered entity changes a privacy practice that is stated in the Notice, and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the Notice revision, if the covered entity has included in the Notice a statement reserving its right to make such a change.

To implement a change in the Notice as provided above, the covered entity shall:

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

B. Document the revised policy or procedure in written or electronic form; and

C. Revise the Notice as required by the policy regarding the Notice to state the changed practice and to make the revised Notice available. The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised Notice.

The covered entity may change a privacy practice that is stated in the Notice, and the related policies and procedures, without having reserved the right to do so, provided that it implements the changes in the same manner as described above and ensures that the change is effective only with respect to PHI created or received after the effective date of the revised Notice.

AR-14 Documentation

Purpose

To establish guidelines for maintaining required documentation of privacy functions

Guidance

A covered entity must maintain in written or electronic form documentation of privacy functions or actions in accordance with the privacy regulations.

The covered entity shall retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

The covered entity shall maintain documentation on the following:

A. Contents and provision of general HIPAA and entity-specific HIPAA training (see guidance AR-01 Training)

B. Current and previous versions of the Notice of Privacy Practices (see guidance AR-03 Notice of Privacy Practices)

C. Titles and offices of those responsible for processing requests for access, amendments, and disclosures (see guidance AR-09 Designation of Privacy Official)

D. Sanctions policy and any sanctions actions undertaken by the covered entity (see guidance AR-10 Sanctions)

E. Items included in the designated record set (see guidance AR-15 Designated Record Set)

F. Breach notification actions, including the investigation, notification analysis, and actions to prevent recurrence (see guidance AR-16 Breach Response and Notification)

G. Requests by individuals for access to their PHI and actions taken to provide the access (see guidance PR-01 Patient Access to Protected Health Information)

H. 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 (see guidance PR-02 Requests for Restrictions on the Use or Disclosure of Protected Health Information)

I. Requests by individuals for confidential communications and the covered entity's response to the request (see guidance PR-03 Requests for Confidential Communications)

J. Disclosures that are to be included in an accounting of disclosures and any accounting reports processed (see guidance PR-04 Accounting of Disclosures)

K. Requests by individuals for amendment of their PHI and the covered entity's response to the request (see guidance PR-05 Amendment of Protected Health Information)

L. Complaints received and the covered entity's response to the complaint (see guidance PR-06 Patient Complaints)

M. Authorizations, revocations, and waivers of authorization, including resolutions of conflicts among authorizations (see guidance UD-03 Authorizations and UD-13 Research)

AR-15 Designated Record Set

Purpose

To establish guidelines for identifying designated record sets

Guidance

The covered entity shall specify the records that make up its designated record set (DRS).

The covered entity shall include in its DRS all medical records, billing records, and other records used to make health care decisions about an individual. The description should note:

A. The specific types of records to be included

B. Their location

C. Their purpose

D. The name or title of the person responsible for the DRS

The covered entity may differentiate between records to be included in the medical record and in the broader DRS.

Records in the DRS are subject to patient rights dealing with access to and amendment of protected health information (see guidance PR-01 Patient Access to Protected Health Information and PR-05 Amendment of Protected Health Information).

AR-16 Breach Response and Notification

Purpose

To establish guidelines for responding to a potential breach of unsecured protected health information ("PHI"),.

Guidance

A covered entity must notify the University Privacy and Information Security Offices immediately upon discovery of any suspected breach of protected health information (PHI), and cooperate with the Offices in the investigation and mitigation processes.

Discovery

A breach must be treated as discovered by the covered entity/business associate (entity) as of the first day on which such breach is known to the entity, or, by exercising reasonable diligence, would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity or who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

Investigation and Notification

Investigation of a potential breach of unsecured PHI will be conducted by the University Privacy Office or, in the alternative, by the covered entity at the direction of the University Privacy Office. The covered entity must cooperate with the University Privacy Office to ensure that all information about the incident is included in the investigation. Cooperation shall include assistance with interviewing of witnesses and/or workforce members, access to documentation and/or materials involved in the potential breach, access to covered entity 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 individuals, the media, or the Secretary, the University Privacy Office shall provide any such notification. If deemed by the University Privacy Office to require urgency because of possible imminent misuse of unsecured PHI, the University Privacy Office, or in the alternative, the covered entity at the direction of the University Privacy Office, 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 a covered entity was serving as a business associate of a covered entity, the (University) covered entity must immediately notify the University Privacy Officeof the breach so that notification in accordance with the terms of the Business Associate Agreement may be provided. Notification to the covered entity as defined in the Business Associate Agreement, and in accordance with the terms of the Business Associate Agreement, will be provided by the University Privacy Office, or in the alternative, by a member of the University's workforce at the direction of the University Privacy Office.

PR-01 Patient Access to Protected Health Information

Purpose

To establish guidelines for responding to patient requests for access to protected health information

Additional Information related to this guidance may be found in UD-05 Disclosures to Personal Representatives

Guidance

A covered entity must permit an individual to request access to inspect, review, or obtain a copy of the protected health information (PHI) related to the individual and maintained in the covered entity's designated record set.

Right of Access

The covered entity may require individuals to make requests for access in writing.

The right of access by an individual who is the subject of the PHI exists, except for:

A. Psychotherapy notes

B. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding

Access to PHI held by Business Associates or Others

If the covered entity does not maintain the PHI that is the subject of the individual's request and knows where the requested information is maintained (e.g., by a Business Associate), the covered entity shall either

A. Inform the individual where to direct the request for access, or

B. Obtain the information from the Business Associate and provide it to the individual.

This access requirement to PHI held by a Business Associates does not apply if the PHI held by the Business Associate is a duplicate of that maintained by the covered entity.

`

Personal Representatives: Verification and Authority

HIPAA permits covered entities to grant access to PHI about an individual to personal representatives of the individual. Covered entities must develop verification protocols to confirm the identity and authority of any person who requests access to PHI of another individual, if the identity or authority of the requestor is not already known.

A. Parents or legal guardians of a minor child – A parent or legal guardian is considered the personal representative of his or her minor child and is allowed access to the medical records concerning the minor child when such access is not inconsistent with State or other law.

   1. Exceptions

      a. 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

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

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

      d. When the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to domestic violence, abuse, or neglect, or that treating the parent or guardian as the child's personal representative could endanger the child

   2. Even in these exceptions, the parent or guardian may have access to the medical records of the minor child related to treatment when State or other applicable law requires or permits such access. **Covered entities shall contact the University Privacy Office if circumstances do not clearly delineate whether access is allowed.**

B. Power of Attorney – A person who has been given a health care power of attorney for an individual will have the right to access the medical records of the individual.

   1. Exception: Such access may be denied when the provider *reasonably believes in his or her professional judgment* that

      a. the individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or

`

b. treating the person holding power of attorney as the individual's personal representative could endanger the individual or would not be in the best interests of the individual

C. Emancipated Minor or Adult – The personal representative of an emancipated minor or adult may have access to PHI of the emancipated minor or adult but the scope of such access depends upon the authority granted to the personal representative by other law.

1. If the personal representative is authorized to make health care decisions in general, then the personal representative may have access to the individual's PHI regarding health care in general.

2. If the personal representative's authority is limited (e.g., to decisions about artificial life support), then the personal representative's access would be limited to the information which may be relevant to making decisions within his or her scope of authority.

3. Exceptions - Such access may be denied when the provider reasonably believes in his or her professional judgment that

a. The emancipated child or adult has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or

b. Granting the personal representative access to the PHI of the emancipated child or adult could endanger the emancipated child or adult or would not be in the best interests of the emancipated child or adult

Timely Action

The covered entity shall act on a request no later than 30 days after receipt of the request.

If the covered entity is unable to take an action required within the time required, the covered entity may extend the time by no more than 30 days, provided that the covered entity, within the time limit set above, notifies the individual in writing of the reasons for the delay and the date by which the covered entity will complete its action on the request.

Provision of Access

If the covered entity grants the request, in whole or in part, it shall inform the individual of the acceptance of the request, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request.

`

Format. The covered entity shall provide the individual with access to the PHI in the form requested by the individual, if it is readily producible in such form, or, if not, in a readable hard copy form or such other format as agreed to by the covered entity and the individual.

If the covered entity maintains PHI electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the PHI in the electronic format requested by the individual, if it is readily producible in such format; or, if not, in a readable electronic format as agreed to by the covered entity and the individual. In addition, at the individual's request, the covered entity shall transmit the copy of PHI directly to another person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.

If an individual requests PHI by email, covered entities are permitted to send unencrypted emails if they have advised the individual of the risk of the email being read by a third party, and the individual still prefers the unencrypted email.

The covered entity may provide the individual with a summary of the PHI requested, in lieu of providing access, or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to the summary or explanation and to the fees imposed, if any.

Fees. Kentucky law provides that individuals may receive one free copy of the medical record without charge. Covered entities may consider maintaining documentation that reflects receipt of the free copy in order to determine when a fee schedule for record requests may apply.

If the individual requests additional copies of the PHI or agrees to a summary or explanation, the covered entity may impose a reasonable, cost-based fee, if the fee includes only the cost of:

A. Labor for copying the PHI requested by the individual whether in paper or electronic form

B. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media

C. Postage, when the individual has requested the information be mailed

D. Preparing an explanation or summary of the PHI, if agreed to by the individual

Denial of Access

If the covered entity denies access to some or all of the requested PHI, the covered entity shall, to the extent possible, give the individual access to any other PHI requested. The covered entity

`

shall provide a timely, written denial to the individual, in accordance with the Timely Action section above. The denial shall be in plain language and contain:

A. The basis for the denial

B. If applicable, a statement of the individual's review rights, and how the individual may exercise such review rights

C. A description of how the individual may complain to the covered entity pursuant to the complaint procedures or to the Secretary (see guidance PR-06 Patient Complaints) pursuant to the procedures in 45 CFR §160.306. The description shall include the name (or title) and telephone number of the contact person or office designated pursuant to guidance AR-09 Designation of Privacy Official.

Unreviewable Grounds for Denial. The covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

A. The PHI meets one of the exceptions to the Right of Access:

1. Psychotherapy notes

2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding

B. A covered health care provider acting under the direction of a correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the individual or other inmates, or the safety of any person who is at the correctional institution or responsible for the transporting of the inmate.

C. An individual's access to PHI created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

D. An individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

E. An individual's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

`

Reviewable Grounds for Denial. The covered entity may deny an individual access with an opportunity for review, in the following circumstances:

A. A licensed health care professional determines, based upon his or her professional judgment, that granting the individual's request for access is likely to cause substantial harm or to endanger the life or physical safety of the individual or another person

B. The PHI included in the request refers to another person and access to or disclosure of the information is likely to cause substantial harm

C. The request is made by a personal representative and the access or disclosure, if granted would likely cause substantial harm

Review of Denial. If the individual has requested a review of a denial, the covered entity shall promptly refer a request for review to a licensed health care professional who was not directly involved in the denial. The reviewer shall determine, within a reasonable period of time, whether or not to deny the access using the standards pertaining to reviewable grounds for denial. The covered entity shall promptly provide written notice to the individual of the determination and take other action as required to carry out the determination.

Documentation

The covered entity shall document the following and retain the documentation in written or electronic form:

A. The designated record sets that are subject to access by individuals; and

B. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

`

PR-02 Requests for Restrictions on the Use or Disclosure of Protected Health Information

Purpose

To establish guidelines for responding to patient requests for restrictions concerning the use or disclosure of protected health information

Guidance

A covered entity must permit an individual to request a restriction on how the covered entity uses or discloses protected health information (PHI) related to the individual.

The covered entity shall permit an individual to request that the covered entity restrict:

A. Uses or disclosures of protected health information (PHI) about the individual to carry out treatment, payment, or health care operations. This may include, for example, requests to not disclose genetic test results, which, if agreed to, could not be shared with other health care providers for the purpose of treating other family members seeking to identify their own genetic health risks.

B. Disclosures permitted under the guidance UD-04 Disclosures to Family, Friends, and Others

The covered entity is not required to agree to a restriction, except it shall comply with the requested restriction if:

A. Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations; and

B. The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

A restriction agreed to by the covered entity cannot be used to prevent uses or disclosures:

A. When required by the Secretary to investigate or determine the covered entity's compliance with the Privacy Rule

B. For facility directories

C. For which an authorization or opportunity to agree or object is not required (see guidance UD-06 through UD-16)

The covered entity that agrees to a restriction shall document the restriction in written or electronic form.

Emergency Treatment

The covered entity that agrees to a restriction may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the treatment, the covered entity may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual.

If restricted PHI is disclosed to a health care provider for emergency treatment, the covered entity shall request that such health care provider not further use or disclose the information.

Terminating a Restriction

A covered entity may terminate a restriction, if:

A. The individual agrees to or requests the termination in writing;

B. The individual orally agrees to the termination and the oral agreement is documented; or

C. The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is

1. Not effective for PHI restricted by request of the individual and the individual has paid the covered entity in full

2. Only effective with respect to PHI created or received after it has so informed the individual.

PR-03 Requests for Confidential Communications

Purpose

To establish guidelines for responding to patient requests for confidential communications

Guidance

A covered entity must accommodate reasonable requests by individuals to receive communications of protected health information (PHI) by alternative means or at alternative locations.

The covered entity may require the individual to make a request for a confidential communication in writing.

The covered entity may condition the provision of a reasonable accommodation on:

A. When appropriate, information as to how payment, if any, will be handled; and

B. Specification of an alternative address or other method of contact.

A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

PR-04 Accounting of Disclosures

Purpose

To establish guidelines for responding to patient requests for an accounting of disclosures

Guidance

Upon request by an individual, a covered entity must provide an accounting of disclosures of protected health information (PHI) related to the individual and maintained in the covered entity's designated record set.

Disclosures are required for:

A. To the Secretary of the Department of Health & Human Services

B. Required by law (e.g. mandated under state law)

C. For public health activities/reporting

D. About victims of abuse, neglect, or domestic violence

E. For health oversight activities (e.g. licensure actions)

F. In response to a court order, subpoena or discovery request

G. For law enforcement

H. To medical examiner/funeral director & for organ donations

I. For research without authorization

J. To avert a serious threat to health or safety

K. Certain specialized gov't functions (e.g. armed forces personnel) – except for national security or intelligence purposes

L. For workers' compensation

M. Disclosures not permitted by HIPAA (e.g. mistakes)

N. Any other disclosure not on the list of exclusions from the accounting requirement (see below)

The accounting shall include all elements required by the regulation (see Attachment PR-04 – Content of the Accounting of Disclosures), except for disclosures:

A. To carry out treatment, payment and health care operations (see guidance UD-02 Treatment, Payment, and Operations)

B. To individuals of PHI about themselves

C. Incident to a use or disclosure otherwise permitted or required by the privacy regulations (see the multiple guidances on Uses and Disclosures)

D. Pursuant to an authorization (see guidance UD-03 Authorizations)

E. To persons involved in the individual's care or other notification purposes (see guidance UD-04 Disclosures to Family, Friends, and Others)

F. For national security or intelligence purposes (see guidance UD-15 Specialized Government Functions)

G. To correctional institutions or law enforcement officials (see guidance UD-15 Specialized Government Functions)

H. As part of a limited data set (see guidance UD-18 Uses and Disclosures of Limited Data Sets)

The Accounting of Disclosure requirement applies to applicable information disclosed orally, electronically, visually, or in writing.

Suspension

The covered entity shall temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official (see guidance UD-09 Health Oversight Activities and UD-11 Law Enforcement) for the time specified by the agency or official if the agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency or official statement is made orally, the covered entity shall:

A. Document the statement, including the identity of the agency or official making the statement;

B. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

C. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Provision of the Accounting

The covered entity shall act on the individual's request for an accounting as follows, no later than 60 days after receipt of such a request.

A. The covered entity shall provide the individual with the accounting requested; or

B. If the covered entity is unable to provide the accounting within the time required, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

   1. The covered entity, within the time limit, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

   2. The covered entity may have only one such extension of time for action on a request for an accounting.

If the covered entity has a Business Associate which holds information subject to the Accounting of Disclosures requirement, the covered entity must either:

A. Provide the individual with the accounting that it obtains from the Business Associate, or

B. Direct the individual to the Business Associate for the relevant information of the request for the Accounting of Disclosures.

Fees

The covered entity shall provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Documentation

The covered entity shall retain written or electronic documentation of the following:

A. The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;

B. The written accounting that is provided to the individual; and

C. The titles of the persons or offices responsible for receiving and processing requests for an accounting.

Attachment PR-04 – Content of the Accounting of Disclosures

Content of the Accounting

The covered entity shall provide the individual with a written accounting that meets the following requirements.

A. The accounting shall include disclosures of PHI that occurred during the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

B. For each disclosure, the accounting shall include:

1. The date of the disclosure;

2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

3. A brief description of the PHI disclosed; and

4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request, if any, for a disclosure required by the Secretary or for which an authorization or opportunity to agree or object is not required (see guidance UD-06 through UD-16).

Multiple Disclosures. If, during the period covered by the accounting, the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose when required by the Secretary or for disclosures for which an authorization or opportunity to agree or object is not required, the accounting may, with respect to such multiple disclosures, provide:

A. The content required above for the first disclosure during the accounting period;

B. The frequency, periodicity, or number of the disclosures made during the accounting period; and

C. The date of the last such disclosure during the accounting period.

Research. If, during the period covered by the accounting, the covered entity has made disclosures of PHI for a particular research purpose (see guidance UD-13 Research) for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

A. The name of the protocol or other research activity;

B. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

C. A brief description of the type of PHI that was disclosed;

D. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

E. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

F. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If the covered entity provides an accounting for research disclosures, and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

PR-05 Amendment of Protected Health Information

Purpose

To establish guidelines for responding to patient requests for an amendment of his or her protected health information

Guidance

A covered entity must consider an individual's request to amend protected health information (PHI) related to the individual and maintained in the covered entity's designated record set.

The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. Attachment PR-05.1 Request for Amendment may be used when requiring the requests in writing.

The covered entity shall act on the individual's request for an amendment no later than 60 days after receipt of such a request. Attachment PR-05.2 Response to Request for Amendment may be used when responding to requests for amendment.

If the covered entity is unable to act on the amendment within the time required, the covered entity may extend the time for such action by no more than 30 days, provided that the covered entity, within the time limit, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. The covered entity may have only one such extension of time for action on a request for an amendment.

Accepting the Amendment

If the covered entity accepts the requested amendment, in whole or in part, the covered entity shall make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

The covered entity shall timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant

persons with whom the amendment needs to be shared. The covered entity shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

A. Persons identified by the individual as having received PHI about the individual and needing the amendment; and

B. Persons, including business associates, that the covered entity knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

Denying the Amendment

The covered entity may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:

A. Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

B. Is not part of the designated record set;

C. Would not be available for inspection by the individual (see guidance PR-01 Patient Access to Protected Health Information);

D. Is accurate and complete.

If the covered entity denies the requested amendment, in whole or in part, the covered entity shall provide the individual with a written denial within the timeframe noted above. The denial shall use plain language and contain:

A. The basis for the denial;

B. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

C. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

D. A description of how the individual may complain to the covered entity (see guidance PR-06 Patient Complaints) or to the Secretary. The description shall include the name (or title) and

telephone number of the person or office to contact (see guidance AR-09 Designation of Privacy Official).

Statement of Disagreement. The covered entity shall permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

Rebuttal Statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity shall provide a copy to the individual who submitted the statement of disagreement.

Recordkeeping. The covered entity shall identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link all existing requests and statements to the designated record set.

Future Disclosures. If a statement of disagreement has been submitted by the individual, the covered entity shall include the material appended regarding the disagreement or an accurate summary of any such information with any subsequent disclosure of the PHI to which the disagreement relates.

If the individual has not submitted a written statement of disagreement, the covered entity shall include the individual's request for amendment and its denial or an accurate summary of such information with any subsequent disclosure of the PHI only if the individual has requested such action.

When a subsequent disclosure is made using a standard transaction (as defined in the HIPAA regulations) that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required to the recipient of the standard transaction.

Actions on Notices of Amendment

The covered entity that is informed by another covered entity of an amendment to an individual's PHI shall amend the PHI in designated record sets as provided above.

Documentation

The covered entity shall document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation in writing or electronically.

Attachment PR-05.1 Request for Amendment

COVERED ENTITY NAME
ADDRESS
ADDRESS
PHONE

Request for Amendment of Medical Record

Patient Name _____ Date of Birth _____

Address _____

Phone _____ Medical Record # _____

Medical Record to Change. I request that a change be made to the following medical record (include information such as date, nature of service received, doctor/staff member seen):

_____

_____

Changes Requested. I request that you make the following change or addition:

_____

_____

Reason. I believe the record needs to be changed because:

_____

_____

Others that I Request You Send the Change to. The following people or offices also need be told about this change (include name and address):

_____

_____

I understand that the covered entity does not have to make this change. I understand that I will be notified within 30 days of the covered entity's decision or of the covered entity's need for further time to decide on this request.

Signature (Patient or Patient's Representative)	Date
Printed Name of Patient's Representative	Relationship to Patient

Attachment PR-05.2 Response to Request for Amendment

COVERED ENTITY NAME
ADDRESS
ADDRESS
PHONE

Response to Request for Amendment of the Medical Record

Patient Name _____ Date of Birth _____

Address _____

Phone _____ Medical Record # _____

We have reviewed your request to change the medical record. Your request was:

_____Accepted

_____Denied because:

_____We believe that the information is accurate and complete.

_____We did not create the information. (If the creator of the information is no longer in business, please let us know, and we will re-assess our decision.)

_____The information is not part of the medical record.

_____Other:_____

_____

Statement of Disagreement. If you disagree with our denial, you may send a written statement giving your reason for disagreeing. The statement should be sent to Contact Name/Title at the address above.

Rebuttal Statement. We may prepare a statement responding to your disagreement. If we do, we will send you a copy.

Complaint. You have the right, if you wish, to complain about the denial to the covered entity or to the Secretary of the US Department of Health and Human Services (HHS). To complain to

the covered entity or ask questions about this process, please contact Contact Name/Title at the address or telephone number above.

To complain to the Secretary, the complaint must:

- Be filed in writing, either on paper or electronically, by mail, fax, or e-mail (see the name and address below, or look on the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html);
- Name the covered entity involved and describe the acts or omissions you believe violated the HIPAA Privacy or Security Rule; and
- Be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause."

Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
Sam Nunn Atlanta Federal Center, Suite 16T70
61 Forsyth Street, S.W.
Atlanta, GA 30303-8909
Voice Phone (404) 562-7886
FAX (404) 562-7881
TDD (404) 562-7884

Future Disclosures. All information pertaining to your request and our response to it (or an accurate summary) will be put with the part of the medical record related to the request. If this record is sent to anyone in the future, the information about your request and our response will be also be sent.

Signature (Covered Entity Contact) Date

Printed Name of Covered Entity Contact

PR-06 Patient Complaints

Purpose

To establish guidelines for responding to patient privacy complaints

Guidance

A covered entity must implement a process for receiving and responding to privacy complaints from individuals.

The process shall include provision of the name (or title) and telephone number of the contact person or office designated pursuant to guidance AR-09 Designation of Privacy Official.

The covered entity shall maintain written or electronic documentation of all complaints received, and their disposition, if any.

The covered entity may not require individuals to waive their rights to complain to the Secretary as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

UD-01 Uses and Disclosures of Protected Health Information

Purpose

To establish guidelines for permitted and required uses and disclosure of protected health information

Guidance

A covered entity must ensure its use or disclosure of protected health information (PHI) is made in accordance with the privacy regulations.

The covered entity is required to disclose PHI:

A. To the individual who is the subject of the information requested (see guidance PR-01 Patient Access to Protected Health Information and PR-04 Accounting of Disclosures)

B. To the Secretary to investigate or determine the covered entity's compliance with the privacy regulations. Disclosures made to the Secretary are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

If the covered entity is functioning as a business associate, it is required to disclose PHI:

A. 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 guidance PR-01 Patient Access to Protected Health Information)

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

The covered entity is permitted to use or disclose PHI as follows:

A. To the individual who is the subject of the information

B. For treatment, payment, or health care operations (see guidance UD-02 Treatment, Payment, and Operations)

C. Incident to a use or disclosure otherwise permitted or required by the privacy regulations, provided that the covered entity follows the regulations on minimum necessary use or disclosure (see guidance AR-05 Minimum Necessary) and has in place appropriate

administrative, technical, and physical safeguards to protect the privacy of PHI (see guidance AR-07 Safeguards for Storage, Transmission, and Disposal of PHI)

D. With a valid authorization (see guidance UD-03 Authorization), except for the prohibited uses and disclosures of genetic information for underwriting purposes

E. To family, friends, and others involved in the individual's care, as long as the individual has the opportunity to object (see guidance UD-04 Disclosures to Family, Friends, and Others)

Sensitive Health Information

If state law provides additional protections to sensitive information, the covered entity shall apply the required protection. Under Kentucky law, for instance, information about HIV status carries additional protections. Without the individual's consent, the covered entity shall share HIV information only with the following persons:

A. the individual,

B. the individual's legally authorized representative,

C. colleagues to determine diagnosis, provide treatment or for consultation,

D. the State under applicable reporting obligations,

E. anyone the individual has designated in a legally effective release executed prior to the information being shared,

F. applicable committees within a health care facility for program monitoring, program evaluations or services reviews,

G. organ procurement organizations,

H. authorized medical or epidemiological researchers, and

I. a person allowed access by court order.

When making this type of disclosure, the covered entity shall also send to the recipient a statement that includes the following language:

"This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of such information without the specific written consent of the person to whom such information pertains, or as

otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for this purpose."

Whistleblowers

The covered entity is not considered to have violated the privacy regulations if:

A. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

B. The disclosure is to:

   1. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

   2. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the good faith conduct described above.

Workforce Member Crime Victims

The covered entity is not considered to have violated the requirements of the privacy regulations if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that the PHI disclosed is:

A. About the suspected perpetrator of the criminal act; and

B. Limited to:

   1. Name and address;

   2. Date and place of birth;

   3. Social security number;

   4. ABO blood type and rh factor;

5. Type of injury;
6. Date and time of treatment;
7. Date and time of death, if applicable; and
8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

UD-02 Treatment, Payment, and Operations

Purpose

To establish guidelines for the use or disclosure of protected health information for treatment, payment, or health care operations purposes

Guidance

A covered entity must ensure its use and disclosure of protected health information (PHI) for purposes of treatment, payment, or health care operations are made in accordance with the privacy regulations.

Except with respect to uses or disclosures of psychotherapy notes, for marketing, or for sale of PHI that require an authorization (see guidance UD-03 Authorization, UD-20 Marketing, and UD-21 Prohibition on Sale of Protected Health Information) or the prohibited uses and disclosures of genetic information for underwriting purposes, the covered entity may use or disclose PHI for treatment, payment, or health care operations as set forth below.

A. The covered entity may use or disclose PHI for its own treatment, payment, or health care operations.

B. The covered entity may disclose PHI for treatment activities of a health care provider.

C. The covered entity may disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information.

D. The covered entity 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 (see Attachment UD-02 – Operations Definition)

    2. For the purpose of health care fraud and abuse detection or compliance.

The covered entity that participates in an organized health care arrangement (OHCA) may disclose PHI about an individual to other participants in the OHCA for any health care operations activities of the OHCA.

The covered entity may obtain consent of the individual to use or disclose PHI to carry out treatment, payment, or health care operations. Consent shall not be effective to permit a use or disclosure of PHI when an authorization is required or when another condition shall be met for such use or disclosure to be permissible.

Attachment UD-02 – Operations Definition

45 CFR § 164.501 Definitions

Health Care Operations (relevant excerpt) – means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment

B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities

UD-03 Authorizations

Purpose

To establish guidelines for the use and disclosure of information with an authorization

Guidance

For a use or disclosure of protected health information (PHI) that requires an authorization, a covered entity must make such use or disclosure in accordance with a valid authorization.

The authorization shall contain all of the elements required by the privacy regulations (see Attachment UD-03 - Checklist for a Valid Authorization). In addition to the required elements, a valid authorization may contain additional elements or information, if they are not inconsistent with the required elements.

When the covered entity obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure shall be consistent with the authorization. The covered entity shall determine the minimum necessary information needed for the purpose and disclose only that information (see guidance AR-05 Minimum Necessary).

If the covered entity seeks an authorization from an individual for a use or disclosure of PHI, the covered entity shall provide the individual with a copy of the signed authorization.

The covered entity shall document and retain any signed authorization in writing or electronically.

Revocation of Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

A. The covered entity has taken action on the authorization; or

B. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

Psychotherapy Notes

The covered entity shall obtain an authorization for any use or disclosure of psychotherapy notes, except:

A. To carry out the following treatment, payment, or health care operations:

   1. Use by the originator of the psychotherapy notes for treatment

   2. Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling

   3. Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual

B. When required by the Secretary to investigate or determine the covered entity's compliance with the privacy regulations

C. When required by law or for health oversight activities with respect to the oversight of the originator of the psychotherapy notes (see guidance UD-06 Required by Law and UD-09 Health Oversight Activities)

D. To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law (see guidance UD-12 Decedent Information)

E. To avert a serious threat to health or safety (see guidance UD-14 To Avert a Serious Threat or Injury)

Defective Authorizations

An authorization is not valid if the document submitted has any of the following defects:

A. The expiration date or event is known by the covered entity to have passed

B. The authorization has not been filled out completely with respect to a required element, if applicable

C. The authorization is known by the covered entity to have been revoked

D. Any material information in the authorization is known by the covered entity to be false

Compound Authorizations

An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

A. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same research study. This exception includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, any compound authorization created must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

B. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

C. An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization, except when the covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.

Prohibition on Conditioning of Authorizations

The covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

A. A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research.

B. 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, if:

   1. The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

   2. The authorization is not for a use or disclosure of psychotherapy notes.

C. The covered entity 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.

Attachment UD-03 - Checklist for a Valid Authorization

A valid authorization to disclose protected health information (PHI) shall be written in plain language and shall contain the following core elements:

_____ A specific and meaningful description of the PHI to be used or disclosed. For research authorizations only, the description may include information about use of PHI for future research.

_____ The identification of the persons or class of persons authorized to make the use or disclosure of PHI (Who do you want to get information from including your own hospital, practice group, etc.?)

_____ The identification of the persons or class of persons to whom the covered entity is authorized to make the disclosure (What internal or external persons or entities will be getting the information?)

_____ Description of each purpose for which the specific PHI identified earlier is to be used or disclosed (When an individual initiates an authorization for their own purposes, the purpose may be stated as "at the request of the individual.")

_____ An expiration date or event (This must be a certain date or an event tied to the individual.). If the authorization is for a use or disclosure of PHI for research, the statement "end of the research study," "none," or similar language is sufficient.

_____ The individual's signature and date, and if signed by a personal representative, a description of his or her authority to act for the individual

In addition to the core elements, the authorization shall contain the following required statements:

_____ The individual may revoke the authorization in writing, and instructions on how to exercise such right (Where does the individual need to write, including name – or title – and address?)

_____ Treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the Privacy Rule or, if conditioning is permitted, a statement about the consequences of refusing to sign the authorization

_____ The potential for the PHI to be redisclosed by the recipient and no longer protected by the Privacy Rule

An authorization is not valid unless it contains all of the required core elements and all of the required statements.

UD-04 Disclosures to Family, Friends, and Others

Purpose

To establish guidelines for disclosures of protected health information to family, friends, and others involved in the individual's care

Guidance

A covered entity must ensure its disclosures of protected health information (PHI) to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, are made in accordance with the privacy regulations.

The PHI disclosed to such persons shall be directly relevant to the person's involvement with the individual's care or payment related to the individual's health care.

If the individual is present for, or otherwise available prior to, a permitted use or disclosure and has the capacity to make health care decisions, the covered entity may use or disclose the PHI if it:

A. Obtains the individual's agreement (may be oral);

B. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

C. Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

Disclosures made under this guidance may be subject to disclosure restrictions requested by the individual and agreed to by the health care provider. For this reason, the University Privacy Office recommends that covered entities focus their documentation efforts toward identifying those with whom the covered entity is not permitted share PHI.

Limited Uses and Disclosures when the Individual is not Present

If the individual is not present, or the opportunity to agree or object cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual. If so, the covered entity shall disclose only the PHI that is directly

relevant to the person's involvement with the individual's health care or payment related to the individual's health care.

In addition, the covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

Notification

The covered entity may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes shall be in accordance with the provisions above, as applicable.

If the individual is deceased, a covered entity may disclose, to a family member or other persons identified above who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

For the purpose of such notification, the covered entity may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The requirements above apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Other Element

The minimum necessary standard applies to PHI disclosed to family, friends and others involved in the care of the individual (see guidance AR-05 Minimum Necessary).

UD-05 Disclosures to Personal Representatives

Purpose

To establish guidelines for disclosures of protected health information to personal representatives.

Additional information related to this guidance may be found in PR-01Patient Access to Protected Health Information.

Guidance

A covered entity must ensure its disclosure of protected health information (PHI) to a personal representative of an individual is made in accordance with the privacy regulations.

The covered entity shall treat a personal representative as the individual with respect to PHI relevant to such personal representation, except as provided below for unemancipated minors and for situations of abuse, neglect, or endangerment.

The covered entity shall treat 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

Covered entities must develop verification protocols to confirm the identity and authority of those who present themselves as personal representatives of an individual who is the subject of PHI maintained by the covered entity, if the identity or authority of the personal representative is not already known.

A. 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 the covered entity must consider parent or legal guardian as the personal representative of the unemancipated minor.

    1. Exceptions

a. 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

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

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

i. When the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to domestic violence, abuse, or neglect, or that treating the parent or guardian as the child's personal representative could endanger the child

B. Power of Attorney – A person who has been given a health care power of attorney for an individual will be considered the personal representative of the individual.

1. Exception: A covered entity may not consider a person to be the personal representative of an individual when the health care provider reasonably believes in his or her professional judgment that

a. the individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or

b. treating the person holding power of attorney as the individual's personal representative could endanger the individual or would not be in the best interests of the individual

C. Emancipated Minor or Adult – A person without a power of attorney may be considered the personal representative of an emancipated minor or adult to the extent the person's authority to serve as such is granted by other law.

1. If the personal representative is authorized to make health care decisions in general, then the covered entity may disclose to the personal representative PHI regarding health care in general of the individual.

2. If the personal representative's authority is limited (e.g., to decisions about artificial life support), then the covered entity may disclose limited PHI relevant to making decisions within his or her scope of authority.

3. Exceptions: Disclosure of PHI may be denied when the provider *reasonably believes in his or her professional judgment* that

a. The emancipated child or adult has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or

b. Disclosing PHI of the emancipated child or adult to the personal representative could endanger the emancipated child or adult or would not be in the best interests. of the emancipated child or adult

UD-06 Required by Law

Purpose

To establish guidelines for disclosure of protected health information when required by law

Guidance

A covered entity must ensure its disclosure of protected health information (PHI) for purposes required by law is made in accordance with the privacy regulations.

The covered entity may use or disclose PHI without the written authorization of the individual and without giving the individual an opportunity to agree or object to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

For uses or disclosures required by law, the covered entity shall meet the requirements described in the guidance UD-08 Victims of Abuse, Neglect, or Domestic Violence; UD-10 Judicial and Administrative Proceedings; or UD-11 Law Enforcement.

Other Element

Disclosures made under the Required by Law exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-07 Public Health Activities

Purpose

To establish guidelines for the use or disclosure protected health information for public health activities

Guidance

A covered entity must ensure its disclosures of protected health information (PHI) for purposes of reporting public health activities are made in accordance with the privacy regulations.

The covered entity may use or disclose PHI without the written authorization of the individual and without giving the individual an opportunity to agree or object for public health activities to:

A. A public health authority that is authorized by law to collect or receive such information for the purpose of reporting, preventing, or controlling disease, injury, or disability; or, 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

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

C. 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:

    1. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations

    2. To track FDA-regulated products

    3. To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback)

    4. To conduct post marketing surveillance

D. 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 covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation

E. An employer, about an individual who is a member of the workforce of the employer, if:

1. The covered entity is a covered health care provider who provides health care to the individual at the employer's request:

    a. To conduct an evaluation relating to medical surveillance of the workplace

    b. To evaluate whether the individual has a work-related illness or injury;

2. The PHI consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

3. The employer needs such findings in order to comply with its obligations, under Occupational Safety and Health Administration regulations, Mine Safety and Health Administration regulations, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

4. The covered health care provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

    a. By giving a copy of the notice to the individual at the time the health care is provided; or

    b. If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

F. A school, about an individual who is a student or prospective student of the school, if:

1. The PHI that is disclosed is limited to proof of immunization;

2. The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

3. The covered entity obtains and documents the agreement to the disclosure from either:

    a. A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

b. The individual, if the individual is an adult or emancipated minor.

If the covered entity also is a public health authority, the covered entity is permitted to use PHI in all cases in which it is permitted to disclose such information for the public health activities described above.

Other Elements

The minimum necessary standard applies to PHI disclosed for Public Health Activities (see guidance AR-05 Minimum Necessary).

Disclosures made under the Public Health Activities exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-08 Victims of Abuse, Neglect, or Domestic Violence

Purpose

To establish guidelines for the use and disclosure of protected health information in cases of abuse, neglect, or domestic violence

Guidance

A covered entity must ensure its disclosures of protected health information (PHI) for purposes of reporting abuse, neglect, or domestic violence are made in accordance with the privacy regulations.

If the covered entity reasonably believes that an individual is a victim of abuse, neglect, or domestic violence, the covered entity may use or disclose PHI to a public health authority or other government authority, including a social service or protective services agency, authorized by law to receive reports of abuse, neglect, or domestic violence:

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

B. If the individual agrees to the disclosure; or

C. To the extent the disclosure is expressly authorized by statute or regulation and:

   1. The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

   2. 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 these circumstances, the PHI may be used or disclosed without the written authorization of the individual and without giving the individual an opportunity to agree or object. The covered entity shall promptly inform the individual that such a report has been or will be made, except if:

A. The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

B. The covered entity would be informing a personal representative, and the covered entity reasonably believes, in the exercise of professional judgment, that the personal representative is responsible for the abuse, neglect, or other injury, and that informing the person would not be in the best interests of the individual.

The covered entity's information and the individual's agreement may be given orally.

This guidance applies for adults only. Refer to guidance UD-07 Public Health Activities for disclosures related to suspected abuse or neglect for children.

Other Elements

The minimum necessary standard applies to PHI disclosed under the Victims of Abuse, Neglect, or Domestic Violence exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the Victims of Abuse, Neglect, or Domestic Violence exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-09 Health Oversight Activities

Purpose

To establish guidelines for the use and disclosure of protected health information for health oversight activities

Guidance

A covered entity must ensure its disclosures of protected health information (PHI) for purposes of health oversight activities are made in accordance with the privacy regulations.

The covered entity may use or disclose PHI without the written authorization of the individual and without giving the individual an opportunity to agree or object to a health oversight agency as authorized by law (including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities) for oversight activities of:

A. The health care system

B. Government benefit programs for which health information is relevant to beneficiary eligibility

C. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards

D. Entities subject to civil rights laws for which health information is necessary for determining compliance

If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity.

For the purpose of the disclosures permitted above, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

A. The receipt of health care

B. A claim for public benefits related to health

C. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services

Other Elements

The minimum necessary standard applies to PHI disclosed under the Health Oversight Activities exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the Health Oversight Activities exception are required to be documented in the Accounting of Disclosures (see guidance on PR-04 Accounting of Disclosures).

UD-10 Judicial and Administrative Proceedings

Purpose

To establish guidelines for the use and disclosure of protected health information for judicial and administrative proceedings

Guidance

A covered entity must ensure its responses to disclosure requests received as part of judicial administrative proceedings are made in accordance with the privacy regulations.

Court Order

The covered entity may disclose protected health information (PHI) without the written authorization of the individual and without giving the individual an opportunity to agree or object in the course of any judicial or administrative proceeding in response to a court order, provided that the covered entity discloses only the PHI expressly authorized by the order.

Covered entities shall contact University Counsel or the University Privacy Office for assistance in determining the validity of or appropriate response to a court order.

Subpoena, Discovery Request, or Other Lawful Process

The covered entity may disclose PHI in response to a subpoena, discovery request, or other lawful process, if the following conditions are met:

A. The covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by the party to:

   1. Ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or

   2. Secure a qualified protective order for the information requested (see Qualified Protective Order section below) **OR**

B. The covered entity itself makes reasonable efforts to

1. Ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or

2. Secure a qualified protective order for the information requested (see Qualified Protective Order section below **AND**

    a. The covered entity must make reasonable efforts to limit the PHI to that which is the minimum necessary to respond to the request.

Receiving satisfactory assurance with regard to a subpoena, discovery request, or other lawful process means the covered entity has obtained a written statement and accompanying documentation demonstrating that:

A. The party requesting the 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; and

C. The time for the individual to raise objections to the court has elapsed, and:

    1. No objections were filed; or

    2. All objections filed by the individual have been resolved by the court and the disclosures being sought are consistent with such resolution.

Qualified Protective Order

A qualified protective order prohibits the parties to the litigation or proceeding from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested. It requires the return of PHI to the covered entity or destruction of the PHI (including copies) at the end of the litigation or proceeding.

Receiving satisfactory assurance with regard to a qualified protective order means the covered entity has obtained a written statement and accompanying documentation demonstrating that:

A. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court with jurisdiction over the dispute; or

B. The party seeking the PHI has requested a qualified protective order from such court.

Disclosures without Satisfactory Assurance

The covered entity may disclose PHI in response to a subpoena, discovery request or other lawful process without receiving satisfactory assurance, if the covered entity makes reasonable efforts to provide notice to the individual or to seek a qualified protective order sufficient to meet the requirements noted above. Covered entities are cautioned to consult with University Counsel or the University Privacy Office before disclosing PHI without the satisfactory assurances described herein.

Other Elements

The minimum necessary standard applies to PHI disclosed under the Judicial and Administrative Proceedings exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the Judicial and Administrative Proceedings exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-11 Law Enforcement

Purpose

To establish guidelines for the use and disclosure of protected health information for law enforcement purposes

Guidance

A covered entity must ensure its disclosures for law enforcement purposes are made in accordance with the privacy regulations.

The covered entity may use or disclose protected health information (PHI) without the written authorization of the individual and without giving the individual an opportunity to agree or object for a law enforcement purpose to a law enforcement official if one of the following conditions is met.

Required by Law

The covered entity may disclose PHI:

A. As required by law, including laws that require the reporting of certain types of wounds or other physical injuries, except for laws pertaining to victims of abuse, neglect, or domestic violence (see guidance UD-08 Victims of Abuse, Neglect, or Domestic Violence); or

B. In compliance with and as limited by the relevant requirements of:

   1. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

   2. A grand jury subpoena; or

   3. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

      a. The information sought is relevant and material to a legitimate law enforcement inquiry;

      b. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

c. De-identified information could not reasonably be used.

Limited Information for Identification and Location Purposes

The covered entity may disclose PHI in response to a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. The covered entity 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, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

For the purposes of identification or location, the covered entity may not disclose any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue.

Victims of a Crime

The covered entity may disclose PHI in response to a law enforcement official's request for PHI about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to guidance UD-07 Public Health Activities and UD-08 Victims of Abuse, Neglect, or Domestic Violence, if:

A. The individual agrees to the disclosure; or

B. The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

1. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and the information is not intended to be used against the victim;

2. The law enforcement official represents that immediate law 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; and

3. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Decedents

For the purpose of alerting law enforcement of the death of the individual, the covered entity may disclose PHI about an individual who has died to a law enforcement official if the covered entity has a suspicion that such death may have resulted from criminal conduct.

Crime on Premises

The covered entity may disclose to a law enforcement official PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

Reporting Crime in Emergencies

A covered health care provider providing emergency health care in response to a medical emergency, other than an emergency on the premises of the covered health care provider, may disclose PHI to a law enforcement official if the disclosure appears necessary to alert law enforcement to:

A. The commission and nature of a crime;

B. The location of the crime or of the victim(s) of the crime; and

C. The identity, description, and location of the perpetrator of the crime.

If a covered health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, the paragraph above does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to guidance UD-08 Victims of Abuse, Neglect, or Domestic Violence.

Note: Information may also be disclosed to avert a serious threat or injury. For additional guidance, see UD-14 To Avert a Serious Threat or Injury.

Other Elements

The minimum necessary standard applies to PHI disclosed for Law Enforcement purposes (see guidance AR-05 Minimum Necessary).

Disclosures made under the Law Enforcement exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-12 Decedent Information

Purpose

To establish guidelines for uses and disclosures of protected health information of decedents

Guidance

A covered entity must ensure its disclosures of protected health information (PHI) of deceased individuals are made in accordance with the privacy regulations for a period of 50 years following the death of the individual.

Coroners and Medical Examiners

The covered entity may use or disclose PHI without the written authorization of the individual and without giving the individual an opportunity to agree or object to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. This includes alerting law enforcement officials of the death of an individual if the covered entity has a suspicion that such death may have resulted from criminal conduct (see guidance UD-11 Law Enforcement). The covered entity that also performs the duties of a coroner or medical examiner may use PHI for the purposes described in this guidance.

Funeral Directors

The covered entity may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes

The covered entity may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Family, Friends, and Others involved in the Care of the Individual prior to Death

See guidance UD-04 Disclosures to Family, Friends, and Others for disclosures of decedent information made to families, friends, and others.

Uses and Disclosures for Research Purposes

See guidance UD-13 Research for using PHI of decedents for research purposes.

Other Elements

The minimum necessary standard applies to PHI disclosed under the Decedent Information exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the exception for Decedent Information are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-13 Research

Purpose

To establish guidelines for how protected health information may be used or disclosed for research purposes

Guidance

A covered entity must ensure its disclosures for research purposes are made in accordance with the privacy regulations.

De-identified Data

Protected health information (PHI) that has been de-identified prior to its use or disclosure for research purposes (see guidance UD-17 Uses and Disclosures of De-Identified Protected Health Information) may be used for research purposes without further restriction under HIPAA.

Limited Data Set

PHI in the form of a limited data set (see guidance UD-18 Uses and Disclosures of Limited Data Sets) may be used for research purposes as long as a data use agreement is in place with the recipient. Note that PHI disclosed for research purposes under the LDS exception cannot include data elements beyond what is allowed under an LDS. If additional data elements are needed, the investigator will need to obtain an Authorization from the research participant or an alteration of authorization (complete waiver or partial waiver) approved by the Institutional Review Board and/or Privacy Board.

Authorization

PHI may be used or disclosed for research purposes with a written valid authorization from the research participant. The covered entity 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 guidance UD-03 Authorization), with the following special provisions:

A. 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.

B. 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 health information related to the type of treatment assigned. The research authorization will indicate whether or not the individual has agreed to waive this right, and the covered entity must be cognizant of the restricted access in the event a request for access is received during the time frame when the waiver applies (see guidance PR-01 Patient Access to Protected Health Information).

If a research participant revokes his or her research authorization, the covered entity may no longer use or disclose the participant's PHI for research purposes. Covered entities must maintain a copy of all authorizations and any corresponding revocations.

Waiver or Alteration of Authorization

PHI may be used or disclosed for research purposes without an authorization from the research participant if the covered entity obtains written documentation from the Institutional Review Board (IRB) or Privacy Board that an alteration of authorization (i.e., "partial waiver") or waiver of authorization (i.e., "complete waiver") has been approved.

HIPAA requires that the IRB or Privacy Board granting such approval meets the following requirements:

A. Has members with varying backgrounds and the appropriate professional competency necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

B. Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

C. Does not have any member participating in a review of any project in which the member has a conflict of interest.

The partial waiver is most commonly used for purposes such as identifying which individuals may be eligible to participate in a particular study or to determine feasibility of the study.

The complete waiver is most commonly used for retrospective records review and similar protocols where there is no opportunity to obtain a research authorization from the individuals.

Unlike the Preparatory to Research exception, PHI accessed or collected under the Waiver or Alteration of Authorization exception may be removed from the covered entity where it was obtained.

Prior to granting access to or releasing PHI to a researcher under the Alteration or Waiver of Authorization exception, the covered entity shall obtain documentation of the IRB or Privacy Board approval of the waiver. This documentation shall contain the elements required by the privacy regulations (see Attachment UD-13.1 - Required Elements, Documentation of Waiver Approval).

Preparatory to Research

Before the covered entity uses or discloses PHI preparatory to research, the entity shall obtain from the researcher the representations required (see Attachment UD-13.2 - Checklist for the Preparatory to Research Exception).

The preparatory to research exception is generally used when a researcher seeks to review information for the purpose of designing a research study or to assess the feasibility of conducting a study.

This exception is rarely used in our University environment because it stipulates that the PHI cannot be removed from the covered entity, and most University researchers need to collect PHI and transfer it to their academic offices for further research analysis and documentation.

PHI may be used or disclosed for research purposes under the preparatory to research exception if the covered entity obtains the following representations from the researcher:

A. The use or disclosure of the PHI is solely to prepare a research protocol or similar purposes preparatory to research, and

B. The researcher will not remove any PHI from the covered entity, and

C. The PHI for which access is sought is necessary for the research purpose

Covered entities may utilize Attachment UD-13.2 - Checklist for the Preparatory to Research Exception template to document uses or disclosures made under this exception.

The minimum necessary standard applies to PHI disclosed under the Preparatory to Research exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the Preparatory to Research exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

Information on Decedents

Before the covered entity uses or discloses PHI for research on decedents, the entity shall obtain from the researcher the representations required (see Attachment UD-13.3 - Checklist for the Research on Decedents Exception). This requirement remains in effect until 50 years after the individual's death, at which point the data are no longer considered PHI under HIPAA.

The Information on Decedents research exception is generally used when a researcher seeks to review PHI of decedents only and cannot include information about living individuals.

PHI may be used or disclosed for research purposes under the Information on Decedents exception if the covered entity obtains the following representations from the researcher:

A. The use or disclosure of the PHI is solely for research on decedents, and

B. The PHI for which access is sought is necessary for the research purpose, and

C. (optional) Documentation of the death of the individuals about whom PHI is sought.

Covered entities may utilize Attachment UD-13.3 - Checklist for the Research on Decedents Exception template to document uses or disclosures made under this exception.

The minimum necessary standard applies to PHI disclosed research on Decedents exception (see guidance AR-05 Minimum Necessary).

Disclosures made under the Information on Decedents research exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

Effect of Prior Permission for Research

The covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, PHI that it created or received either before or after the applicable compliance date of the privacy regulations, provided that there is no agreed-to restriction (see guidance PR-02 Requests for Restrictions on the Use or Disclosure

of Protected Health Information), and the covered entity obtained, prior to the applicable compliance date, either:

A. An authorization or other express legal permission from an individual to use or disclose PHI for the research;

B. The informed consent of the individual to participate in the research; or

C. A waiver, by an IRB, of informed consent for the research, provided that the covered entity shall obtain authorization (see guidance UD-03 Authorization) if, after the compliance date, informed consent is sought from an individual participating in the research.

Attachment UD-13.1 - Required Elements, Documentation of Waiver Approval

For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation shall include all of the following:

Identification and Date of Action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved

Waiver Criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

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

   1. An adequate plan to protect the identifiers from improper use and disclosure;

   2. 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

   3. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required 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 regulations;

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.

Protected Health Information Needed. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board

Review and Approval Procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

A. An IRB shall follow the requirements of the Common Rule, including the normal review or the expedited review procedures.

B. A privacy board shall review the proposed research at convened meetings at which a majority of the privacy board members are present and the alteration or waiver of authorization shall be approved by the majority of the privacy board members present at the meeting, unless the

privacy board elects to use an expedited review procedure. At least one member shall be present who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities.

C. A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair.

Required Signature. The documentation of the alteration or waiver of authorization shall be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

Attachment UD-13.2 - Checklist for the Preparatory to Research Exception

Name of Researcher _____

Date _____

Study Name or Description _____

_____

_____

HIPAA permits the use or disclosure of PHI held by a covered entity for purposes preparatory to research if the covered entity obtains verbal or written representations from the researcher that:

_____ The use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research

_____ The researcher will not remove any PHI from the covered entity in the course of the review

_____ The PHI for which access is sought is necessary for the research purpose

Do not use this form if a partial waiver, complete waiver, or research authorization has been obtained.

Attachment UD-13.3 - Checklist for the Research on Decedents Exception

Name of Researcher _____

Date _____

Study Name or Description _____

_____

_____

HIPAA permits the use or disclosure of PHI held by a covered entity for the purpose of research on decedents if the covered entity obtains verbal or written representations from the researcher that:

_____ The use or disclosure being sought is solely for research on the PHI of decedents
_____ The PHI being sought is necessary for the research purpose
_____ (optional) Documentation of the death of the individual(s) about whom PHI is sought

Do not use this form if a partial waiver, complete waiver, or research authorization has been obtained.

UD-14 To Avert a Serious Threat or Injury

Purpose

To establish guidelines for the use and disclosure of protected health information to avert a serious threat or injury

Guidance

A covered entity must ensure its disclosures made to avert a serious threat or injury are made in accordance with the privacy regulations.

The covered entity may use or disclose protected health information (PHI) without the written authorization of the individual and without giving the individual an opportunity to agree or object if the covered entity, in good faith, believes the use or disclosure:

A. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

B. Is necessary for law enforcement authorities to identify or apprehend an individual:

   1. Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

   2. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

The covered entity that uses or discloses PHI is presumed to have acted in good faith with regard to a belief, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

The disclosure shall contain only the statement made by the individual, if relevant, and 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, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

NOTE: In January 2013, the Director of the Office for Civil Rights published a message emphasizing the ability of a health care provider to release information as described above. Specifically, the message notes that information can be released "when a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others." It notes that HIPAA permits the release to police, family, and "others who may be able to intervene to avert harm from the threat."

Use or Disclosure not Permitted

A use or disclosure may not be made if the information is learned by the covered entity:

A. In the course of counseling, therapy, or of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure; or

B. Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described above.

Other Elements

The minimum necessary standard applies to uses and disclosures made under the exception To Avert a Serious Threat or Injury (see guidance AR-05 Minimum Necessary).

Disclosures made under the exception To Avert a Serious Threat or Injury are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-15 Specialized Government Functions

Purpose

To establish guidelines for the use or disclosure of protected health information for specialized government functions

Guidance

A covered entity must ensure its disclosures for purposes of specialized government functions are made in accordance with the privacy regulations.

The covered entity may use or disclose protected health information (PHI) without the written authorization of the individual and without giving the individual an opportunity to agree or object for the following specialized government functions.

Military and Veterans Activities

Armed Forces Personnel. The covered entity may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:

A. Appropriate military command authorities; and

B. The purposes for which the PHI may be used or disclosed.

Veterans. The covered entity that is a component of the Department of Veterans Affairs may use and disclose PHI to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

Foreign Military Personnel. The covered entity may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register.

National Security and Intelligence Activities

The covered entity may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

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

Protective Services for the President and Others

The covered entity 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 (protection by the Secret Service), or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3) (special agents of the Department of State and the Foreign Service), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President or Vice-Present – past, present, or future, including candidates – and their immediate families).

Correctional Institutions and Other Law Enforcement Custodial Situations

The covered entity may disclose PHI about an individual to a correctional institution or a law enforcement official having lawful custody of the inmate or other individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:

A. The provision of health care to the individuals;

B. The health and safety of the individual or other inmates;

C. The health and safety of the officers or employees of or others at the correctional institution;

D. The health and safety of the individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

E. Law enforcement on the premises of the correctional institution; and

F. The administration and maintenance of the safety, security, and good order of the correctional institution.

For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

Disclosures made under this section are *not* required to be documented in the Accounting of Disclosures.

Covered Entities that are Government Programs Providing Public Benefits

A covered entity that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

Other Elements

The minimum necessary standard applies to PHI disclosed for Specialized Government Functions (see guidance AR-05 Minimum Necessary).

Unless otherwise noted, disclosures made under the Specialized Government Functions exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-16 Worker's Compensation

Purpose

To establish guidelines for the use and disclosure of protected health information for worker's compensation purposes

Guidance

A covered entity must ensure its disclosures for purposes of worker's compensation are made in accordance with the privacy regulations.

The covered entity may use or disclose protected health information (PHI) without the written authorization of the individual and without giving the individual an opportunity to agree or object as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

The information disclosed must be directly related to the event from which the claim arises.

Other Elements

The minimum necessary standard applies to disclosures made for worker's compensation purposes (see guidance AR-05 Minimum Necessary).

Disclosures made under the Worker's Compensation exception are required to be documented in the Accounting of Disclosures (see guidance PR-04 Accounting of Disclosures).

UD-17 Uses and Disclosures of De-Identified Protected Health Information

Purpose

To establish guidelines for use or disclosure of de-identified protected health information

Guidance

The covered entity may use protected health information (PHI) to create information that is not individually identifiable health information or disclose PHI only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

Health information that meets the specifications for de-identification (see Attachment UD-17 - De-Identified Data Set) is considered not to be individually identifiable health information, i.e., it is de-identified. The requirements of the privacy regulations do not apply to information that has been de-identified, provided that:

A. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of PHI; and

B. If de-identified information is re-identified, the covered entity may use or disclose such re-identified information only as permitted or required by the privacy regulations.

Requirements for De-identification of PHI

If health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual, the information is not individually identifiable health information. The covered entity may determine that health information is not individually identifiable health information only if:

A. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

   1. By applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

2. Documents the methods and results of the analysis that justify such determination; or

B. The identifiers of the individual or of relatives, employers, or household members of the individual, are removed (see Attachment UD-17 - De-Identified Data Set).

Re-identification

The covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

A. 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

B. 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.

Attachment UD-17 - De-Identified Data Set

To qualify as a de-identified data set, the following identifiers of the individual or of relatives, employers, or household members of the individual, shall be removed. In addition, the covered entity shall not have actual knowledge that the information could be used alone or in combination with other information to identify the subject of the information.

A. Names;

B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

   1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

   2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.

   C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

D. Telephone numbers;

E. Fax numbers;

F. Electronic mail addresses;

G. Social security numbers;

H. Medical record numbers;

I. Health plan beneficiary numbers;

J. Account numbers;

K. Certificate/license numbers;

L. Vehicle identifiers and serial numbers, including license plate numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers;

P. Biometric identifiers, including finger and voice prints;

Q. Full face photographic images and any comparable images; and

R. Any other unique identifying number, characteristic, or code, except the code permitted for re-identification purposes

UD-18 Uses and Disclosures of Limited Data Sets

Purpose

To establish guidelines for use or disclosure of limited data sets

Guidance

Whether or not the limited data set is to be used by the covered entity, the covered entity may use protected health information (PHI) to create a limited data set or disclose PHI only to a business associate for such purpose. The covered entity may use or disclose a limited data set only for the purposes of research, public health, or health care operations.

A limited data set is PHI that excludes the direct identifiers of the individual or of relatives, employers, or household members of the individual (see Attachment UD-18.1 - Limited Data Set).

To use or disclose a limited data set, the covered entity shall enter into a valid data use agreement with the limited data set recipient (see Attachment UD-18.2 - Data Use Agreement) noting that the recipient will only use or disclose the PHI for limited purposes.

If the covered entity knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, the covered entity shall take reasonable steps to cure the breach or end the violation, and, if such steps were unsuccessful:

A. Discontinue disclosure of PHI to the recipient, and

B. Report the problem to the Secretary.

The covered entity that is a limited data set recipient and that violates a data use agreement will be in noncompliance with the requirements of the privacy regulations dealing with limited data sets.

Attachment UD-18.1 - Limited Data Set

To qualify as a limited data set, the following identifiers of the individual or of relatives, employers, or household members of the individual, shall be removed.

A. Names;

B. Postal address information (information that *is allowed* in a limited data set: town, city, precinct level, state, 5-digit zip code)

C. Telephone numbers;

D. Fax numbers;

E. Electronic mail addresses;

F. Social security numbers;

G. Medical record numbers;

H. Health plan beneficiary numbers;

I. Account numbers;

J. Certificate/license numbers;

K. Vehicle identifiers and serial numbers, including license plate numbers;

L. Device identifiers and serial numbers;

M. Web Universal Resource Locators (URLs);

N. Internet Protocol (IP) address numbers;

O. Biometric identifiers, including finger and voice prints; and

P. Full face photographic images and any comparable images.

All elements of *dates are allowed* in a limited data set.

Attachment UD-18.2 - Data Use Agreement

A data use agreement between the covered entity and the limited data set recipient shall:

A. Establish the permitted uses and disclosures of such information by the limited data set recipient (research, public health, or health care operations). The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of the privacy regulations, if done by the covered entity;

B. Establish who is permitted to use or receive the limited data set; and

C. Provide that the limited data set recipient will:

1. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

2. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

3. Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

4. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

5. Not identify the information or contact the individuals.

UD-19 Fundraising

Purpose

To establish guidelines for uses and disclosures of protected health information for fundraising

Guidance

A covered entity must ensure its disclosures for fundraising purposes are made in accordance with the privacy regulations.

For the purpose of raising funds for its own benefit, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information (PHI) without an authorization:

A. Demographic information, which includes name, address, other contact information, age, gender, and date of birth;

B. Dates of health care provided to an individual;

C. Department of service information;

D. Treating physician;

E. Outcome information; and

F. Health insurance status.

The covered entity may not use or disclose PHI for fundraising purposes unless a statement is included in the covered entity's Notice of Privacy Practices that the covered entity may contact the individual for this purpose and that the individual has the right to opt out. The covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

In any fundraising materials it sends to an individual, the covered entity shall include a clear and conspicuous description of how the individual may opt out of future 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. When an individual elects not to receive any further such communication, the covered entity shall treat it as a revocation of authorization.

UD-20 Marketing

Purpose

To establish guidelines for communications with individuals for marketing purposes

Guidance

A covered entity must ensure its disclosures for marketing purposes are made in accordance with the privacy regulations.

The covered entity shall obtain an authorization for any use or disclosure of protected health information (PHI) for marketing, except if the communication is in the form of:

A. A face-to-face communication made by the covered entity to an individual; or

B. A promotional gift of nominal value provided by the covered entity.

If the marketing involves financial remuneration (see definition of Marketing) to the covered entity from a third party, the authorization shall state that such remuneration is involved.

UD-21 Prohibition on Sale of Protected Health Information

Purpose

To establish guidelines for prohibition on the sale of protected health information

Guidance

A covered entity must adhere to the privacy regulations with regard to any remuneration received in exchange for protected health information (PHI).

Except as provided below, the covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any PHI of an individual unless the covered entity obtained a valid authorization from the individual stating that the disclosure will result in remuneration to the covered entity.

Exceptions

The paragraph above shall not apply when the purpose of the exchange is:

A. For public health activities (see guidance UD-07 Public Health Activities).

B. For research (see guidance UD-13 Research) 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.

C. For treatment and payment purposes (see guidance UD-02 Treatment, Payment, and Operations).

D. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for the due diligence related to such activity (see definition of Health Care Operations and guidance UD-02 Treatment, Payment, and Operations).

E. 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 (see guidance AR-04 Business Associates), 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.

F. To provide an individual with a copy of their PHI (see guidance PR-01 Patient Access to Protected Health Information and PR-04 Accounting of Disclosures).

G. Required by law (see guidance UD-06 Required by Law).

H. 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 PHI for such purpose or a fee otherwise expressly permitted by other law.