

## UNIVERSITY OF WYOMING

### HIPAA POLICY 2.1

#### DEFINITIONS OF TERMS

- I. **PURPOSE:** The purpose of this policy is to provide definitions for terms used through the UW HIPAA policies and procedures, which apply to all UW Covered Components. The following terms and acronyms have the definitions and meanings set forth below; however, in the event that any definition below differs from the definitions provided by HIPAA the definitions of HIPAA set forth by HIPAA shall govern.
  
- II. **DEFINITIONS- General:**
  - a. **Accounting of disclosures:** A written record of certain disclosures of personal health information (PHI) that may be required to be maintained and provided to a requesting individual under certain prescribed circumstances.
  - b. **AIDS:** Acquired Immunodeficiency Syndrome.
  - c. **Authorization:** A written document completed and signed by the individual that generally allows use and disclosure of PHI for purposes other than treatment, payment or healthcare operations.
  - d. **Breach:** The acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. There is a presumption that a breach occurred unless one of the three articulated exceptions applies pursuant to 45 C.F.R. 164.402(1).
  - e. **Business Associate (“BA”):** A person, entity, company or organization that is not a member of the University of Wyoming healthcare component’s workforce and yet performs a function or activity on behalf of the University of Wyoming healthcare component that involves the use or disclosure of PHI. This term has broad applicability and includes, other than a health care provider’s employees, “partners” that may provide legal, actuarial, accounting, consulting, data aggregation, management, administration or financial services wherein the services require the disclosure of individually identifiable health information.
  - f. **Correctional Institution:** Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.
  - g. **Covered component (UW):** Any department, school or office or any other unit within the University of Wyoming which is subject to HIPAA and the University of Wyoming HIPAA policies, which includes both the health care components and business associate-like components within the University of Wyoming as designated by the University in Presidential Directive PD3-2015-1, “HIPAA Hybrid entity Designation.”

- h. **Covered Entity:** (1) a health plan (2) a health clearinghouse; and/or (3) a health care provider that transmits any health information in electronic form in connection with a covered transaction covered by HIPAA. The Privacy and Security Rules apply only to “Covered Entities.” Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules’ requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If an entity is not a covered entity, it does not have to comply with the Privacy Rule or the Security Rule.
- i. **Covered functions:** Those functions of an entity the performance of which makes the entity a health plan, health care provider, or health clearinghouse (that is, the function makes the entity a “Covered Entity” subject to HIPAA).
- j. **Covered Transaction:** A transaction for which the Secretary has adopted a standard under HIPAA. It is the transmission of information between two parties to carry out financial or administrative
- k. **Decedent:** Decedent is a term used chiefly in law to describe “a deceased person.”
- l. **Data aggregation:** With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.
- m. **Data breach:** A use or disclosure of unsecured PHI as described in 45 C.F.R. Section 164.400 *et seq.*
- n. **De-identified information:** Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. De-identified information is not subject to the HIPAA Privacy Rule.
- o. **Designated record set:** a group of records maintained by or for a covered entity that is:
  - i. Medical and billing records used by a covered entity to make decisions about an individual;
  - ii. Information about health plan enrollment, payment, claims adjudication, and case or medical management record systems; or
  - iii. Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - iv. For purposes of this definition, the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a covered entity.
- p. **Direct Treatment Relationship:** A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. (See definition of “indirect treatment relationship”) Typically, this involves a face-to-face or direct contact relationship.
- q. **Disclosure of PHI:** The release, transfer, provision of access to, or divulging in any other manner of any Protected Health Information outside the entity holding the information.

- r. **Electronic media:** electronic storage media on which data is or may be stored electronically, including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, Extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Transmissions via paper, facsimile or voice via telephone are not considered to be transmissions via electronic media, if the information exchanged did not exist in electronic form immediately before the transmission
- s. **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: (1) 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 (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
- t. **Health care component:** A component or combination of components of a hybrid entity designated and documented by the hybrid entity. The health care component must include any component that would meet the definition of a covered entity if it were a separate legal entity. The health care component may also include a component only to the extent it performs covered functions or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities. The health care components of the University of Wyoming are listed in the University's Presidential Directive PD3-2015-1, "HIPAA Hybrid Entity Designation."
- u. **Health care operations:** Any of the following activities of a covered entity to the extent the activities are related to covered functions:
  - i. Conducting quality assessment and improvement activities;
  - ii. Reviewing the competence or qualifications of health care professionals, evaluating provider performance and conducting training programs;
  - iii. Underwriting, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance;
  - iv. Conducting or arranging for medical review, legal services and auditing functions;
  - v. Business planning and development;
  - vi. Business management and general administrative duties of the entity;
  - vii. Patient safety activities;
  - viii. Population based activities relating to improving health or reducing health care costs;
  - ix. Protocol development, case management and care coordination;
  - x. Contacting of health care providers and patients with information about treatment.

- v. **Health care provider:** A provider of services as defined by 45 C.F.R. Section 160.103. A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
- w. **Health information:** Any information, whether or recorded in any form or medium that:
  - i. 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
  - ii. Relates to the past, present or future, physical, or mental health 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.
- x. **Health plan:** An individual or group plan that provides, or pays the cost of, medical care as defined at 45 C.F.R. Section 160.103.
- y. **HHS:** U.S. Department of Health and Human Services.
- z. **HIPAA:** The Health Insurance Portability and Accountability Act of 1996, as amended (see 42 U.S.C. Section 1320d et seq).
- aa. **Hybrid Entity:** A single entity that is a covered entity whose business activities include both covered and non-covered functions and who designates health care components in accordance with the regulations. The University of Wyoming is a hybrid entity.
- bb. **Indirect treatment relationship:** A relationship between an individual and a health care provider in which: The health care provider delivers health care to the individual based on the orders of another health care provider; and 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.
- cc. **Individual:** The term individual shall have the same meaning as the term “individual” in 45 C.F.R. Section 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. Section 164.502(g).
- dd. **Individually identifiable health information:** Information that is a subset of health information, including demographic information collected from an individual, and:
  - i. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - ii. 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
    - 1. That identifies the individual; or
    - 2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- ee. **Inmate:** A person incarcerated or otherwise confined to a correctional institution.
- ff. **Law Enforcement:** 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:
  - i. Investigate or conduct an official inquiry into a potential violation of law; or
  - ii. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

gg. **Limited data set:** PHI that excludes direct identifiers of individuals or of their relatives, employers or household members. A limited data set is subject to the HIPAA Privacy Rule and requires a Data Use Agreement prior to release of the data set for internal and external uses and disclosures. The elements of the limited data set are set forth at 45 C.F.R. Section 164.514.

hh. **Marketing:**

- i. Except as provided in paragraph (ii) 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.
- ii. 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.
    - d. 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.
- ii. **Medical Record:** As used throughout the UW HIPAA Policies, medical record includes not only the hard copies of the patient's medical treatment and history, but also includes any electronic (digital) version of this same information in an Electronic Medical

Record (EMR) or may include the patient's Electronic Health Records (EHR) which includes information from all clinicians involved in the patient's care.

jj. **Minimum necessary:** The standard for uses and disclosures of PHI. Unless a specific exclusion applies, the general standard is that only the minimum necessary PHI may be used or disclosed to achieve the intended purposes of the use or disclosure.

kk. **Payment:**

i. The activities undertaken by:

1. Except for genetic information in underwriting which is prohibited, 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

ii. The activities in paragraph (i.) of this definition 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.

ll. **Privacy Rule:** The standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and part 164, Subparts A and E.

mm. **Protected health information (PHI):** Individually identifiable health information that is maintained in any medium or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records covered by the

Family Educational Rights and Privacy Act (FERPA) and records held by a covered entity in its role as an employer.

- nn. **Psychotherapy notes:** Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and *that are separated from the rest of the individual's medical record*. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- oo. **Required by law:** A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- pp. **Research:** A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
- qq. **Secretary:** The term "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.
- rr. **Security Rule:** The Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C.
- ss. **Transaction:** The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
  - i. Health care claims or equivalent encounter information.
  - ii. Health care payment and remittance advice.
  - iii. Coordination of benefits.
  - iv. Health care claim status.
  - v. Enrollment and disenrollment in a health plan.
  - vi. Eligibility for a health plan.
  - vii. Health plan premium payments.
  - viii. Referral certification and authorization.
  - ix. First report of injury.
  - x. Health claims attachments.
  - xi. Other transactions that the Secretary may prescribe by regulation.
- tt. **Treatment:** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation

between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

- uu. **Unsecured protected health information/PHI:** PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary.
- vv. **Use:** With respect to individually identifiable health information, use means the sharing, employment, application, utilization, examination or analysis or such information within an entity that maintains such information.
- ww. **Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

### III. **DEFINITIONS- Specific to Security:**

- a. **Access:** The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in this subpart, not as used in subparts D or E of this part.)
- b. **Administrative safeguards:** Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
- c. **Authentication:** The corroboration that a person is the one claimed.
- d. **Availability:** The property that data or information is accessible and useable upon demand by an authorized person.
- e. **Confidentiality:** The property that data or information is not made available or disclosed to unauthorized persons or processes.
- f. **Electronic protected health information (ePHI):** Any electronic information that can be used to identify an individual and that was created, used or disclosed in the course of providing health care. PHI excludes individually identifiable information in education records covered by the Family Educational Rights and Privacy Act (FERPA) and records held by a covered entity in its role as an employer.
- g. **Encryption:** The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- h. **Facility:** The physical premises and the interior and exterior of a building(s).
- i. **Firewall:** Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.
- j. **Information system:** An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
- k. **Integrity:** The property that data or information have not been altered or destroyed in an unauthorized manner.

- l. **Malicious software:** Software, for example, a virus, designed to damage or disrupt a system.
- m. **Password:** Confidential authentication information composed of a string of characters.
- n. **Physical safeguards:** Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- o. **Security or Security measures:** All of the administrative, physical, and technical safeguards in an information system.
- p. **Security incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- q. **Technical safeguards:** The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
- r. **User:** A person or entity with authorized access.
- s. **Workstation:** An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Revised August 2015