

## **HIPAA Policies Procedures and Forms Manual**

### **I. Introduction**

#### ***A. General Policy***

Pepperdine University is committed to protecting the privacy of individual health information in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations promulgated there under. These policies and procedures apply to protected health information created, acquired, or maintained by the designated covered components of the University after April 14, 2003. The statements in this Manual represent the University's general operating policies and procedures. For further details regarding these policies and procedures see 45 C.F.R. Parts 160 and 164.

#### ***B. Scope***

Pepperdine University is a hybrid entity as defined in 45 C.F.R. § 164.103 and includes both covered and non-covered components. These policies and procedures apply only to the University's designated covered components, which include:

- Student Health Center;
- Athletic Training Center;
- Student Counseling;
- Pepperdine Psychology and Educational Clinic;
- Pepperdine Community Counseling Center;
- Pepperdine Jerry B.H. Union Rescue Clinic; and
- Center for Human Resources, Benefits Department.

Certain administrative and/or support offices may also be designated as covered components.

The designated covered components may not share protected health information with the non-covered components of the University, unless specifically permitted by the privacy regulations. It is the responsibility of each designated covered component to assure that their employees, students, volunteers, etc. comply with these policies and procedures. A designated covered component may develop and incorporate additional policies and procedures if doing so is necessary and appropriate to comply with more stringent state laws.<sup>1</sup> However, a designated covered component may not delete sections of these policies and procedures without first consulting the Privacy Official or the Security Official.

---

<sup>1</sup> HIPAA ensures a federal standard (a "floor") of privacy protections. State privacy laws may be more stringent than the HIPAA privacy rule. In those cases, the more stringent state law will apply.

## II. Table of Contents

|  |    |
|--|----|
| PEPPERDINE UNIVERSITY .....  | 1  |
| I. Introduction.....   | 1  |
| A. General Policy.....   | 1  |
| B. Scope.....  | 1  |
| II. Table of Contents .....  | 2  |
| III. Definitions.....  | 4  |
| IV. General Policies and Procedures.....                                     | 7  |
| A. Authorization to Use or Disclose Protected Health Information .....       | 7  |
| 1. Policy .....  | 7  |
| 2. Procedure .....   | 8  |
| 3. Applicable Regulation .....   | 9  |
| B. Business Associates .....   | 9  |
| 1. Policy .....  | 9  |
| 2. Procedure .....   | 9  |
| 3. Applicable Regulation .....   | 9  |
| C. Complaint.....  | 9  |
| 1. Policy .....  | 9  |
| 2. Procedure .....   | 10 |
| 3. Applicable Regulation .....   | 10 |
| D. De-Identification of Protected Health Information.....                    | 10 |
| 1. Policy .....  | 10 |
| 2. Procedure .....   | 11 |
| 3. Applicable Regulation .....   | 12 |
| E. Limited Data Sets.....  | 12 |
| 1. Policy .....  | 12 |
| 2. Procedure .....   | 12 |
| 3. Applicable Regulation .....   | 13 |
| F. Minimum Necessary Use and Disclosure of Protected Health Information..... | 13 |
| 1. Policy .....  | 13 |
| 2. Procedure .....   | 13 |
| 3. Applicable Regulation .....   | 14 |
| G. Notice of Privacy Practices.....  | 14 |
| 1. Policy .....  | 14 |
| 2. Procedure .....   | 14 |
| 3. Applicable Regulation .....   | 15 |
| H. Privacy Official.....   | 15 |
| 1. Privacy Coordinator .....   | 16 |
| 2. Security Official.....  | 16 |
| 3. Applicable Regulation .....   | 18 |
| I. Records Retention.....  | 18 |
| 1. Policy .....  | 18 |
| 2. Procedure .....   | 18 |
| 3. Applicable Regulation .....   | 19 |
| J. Research.....   | 19 |
| 1. Policy .....  | 19 |

|    |   |    |
|----|---|----|
| 2. | Procedure .....   | 19 |
| 3. | Applicable Regulation .....   | 21 |
| K. | Right to Request Access to Protected Health Information .....                                 | 21 |
| 1. | Policy .....  | 21 |
| 2. | Procedure .....   | 21 |
| 3. | Applicable Regulation .....   | 23 |
| L. | Right to Request an Accounting of Disclosures .....   | 24 |
| 1. | Policy .....  | 24 |
| 2. | Procedure .....   | 24 |
| 3. | Applicable Regulation .....   | 25 |
| M. | Right to Request an Amendment to Protected Health Information .....                           | 25 |
| 1. | Policy .....  | 25 |
| 2. | Procedure .....   | 26 |
| 3. | Applicable Regulation .....   | 27 |
| N. | Right to Request Confidential Communications .....  | 27 |
| 1. | Policy .....  | 27 |
| 2. | Procedure .....   | 27 |
| 3. | Applicable Regulation .....   | 28 |
| O. | Right to Request Restrictions on the Use and Disclosure of Protected Health Information ..... | 28 |
| 1. | Policy .....  | 28 |
| 2. | Procedure .....   | 28 |
| 3. | Applicable Regulation .....   | 28 |
| P. | Safeguarding Protected Health Information .....   | 28 |
| 1. | Policy .....  | 28 |
| 2. | Procedure .....   | 29 |
| 3. | Applicable Regulation .....   | 29 |
| Q. | Training .....  | 29 |
| 1. | Policy .....  | 29 |
| 2. | Procedure .....   | 30 |
| 3. | Applicable Regulation .....   | 30 |
| V. | HIPAA Sample Forms [see following pages] .....  | 31 |
| A. | Accounting for Disclosures of PHI .....   | 31 |
| B. | Authorization to Use/Disclose PHI .....   | 31 |
| C. | Business Associate Agreement .....  | 31 |
| D. | Denial of Request for Amendment .....   | 31 |
| E. | Denial of Request for Access .....  | 31 |
| F. | Privacy Complaint .....   | 31 |
| G. | Request for Access to PHI .....   | 31 |
| H. | Request for Accounting of Disclosures .....   | 31 |
| I. | Request for Amendment to PHI .....  | 31 |
|    | Pepperdine University .....   | 32 |

### **III. Definitions**

*Business Associate* means a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business Associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity. 45 C.F.R. § 160.103.

*Covered Entity* means a health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted a standard. 45 C.F.R. § 160.103.

*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. 45 C.F.R. § 164.103.

*Designated Covered Components* (or Covered Components) means a component or combination of components designated by the University, which is a Hybrid Entity. The designated covered components of the University are listed in Section I.B. of this Manual.

*Designated Record Set* means a group of records maintained by or for a covered entity that includes medical and billing records about individuals, or a group of records that are used in whole or in part by or for the covered entity to make decisions about individuals. 45 C.F.R. § 164.501.

*Direct Treatment Relationship* means a treatment relationship between an individual and a healthcare provider that is not an indirect treatment relationship. 45 C.F.R. § 164.501.

*Disclosure* means the release, transfer, access to, or divulging of information in any other manner outside the entity holding the information. 45 C.F.R. § 160.103.

*Electronic Media* means electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the internet (wide-open), extranet (using internet technology to

link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile, and of voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission. 45 C.F.R. § 160.103

*HHS* stands for the Department of Health and Human Services.

*Health Care* means care, services, or supplies related to the health of an individual, including (1) preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, services, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual 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. 45 C.F.R. § 160.103.

*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: (1) 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; (2) 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. 45 C.F.R. § 160.103.

*Health Care Operations* means any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment; (2) reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health care providers, training of professionals that are not health care providers, accreditation, certification, licensing, or credentialing activities; (3) underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or benefits; (4) conducting or arranging for medical review, legal services, and auditing functions; (5) business planning and development, and (6) business management and general administrative activities of the entity. 45 C.F.R. § 164.501.

*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. 45 C.F.R. § 160.103.

*Health Information* means any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or University, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. 45 C.F.R. § 160.103.

*Health Plan* means, with certain exceptions, 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)). 45 C.F.R. § 160.103.

*Hybrid Entity* means a single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. 45 C.F.R. § 164.103.

*Indirect Treatment Relationship* means a relationship between an individual and a health care provider in which (1) the health care provider delivers health care to the individual based on the orders of another health care provider; and (2) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. 45 C.F.R. § 164.501.

*Individually Identifiable Health Information* means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care of an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

*Person* means any natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private. 45 C.F.R. § 160.103.

*Protected Health Information (or PHI)* means individually identifiable information transmitted or maintained in electronic media (ePHI), or transmitted or maintained in any form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. 45 C.F.R. §§ 164.501, 160.103.

*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 records. 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. 45 C.F.R. § 164.501.

*Research* means a systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge. 45 C.F.R. § 164.501.

*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. 45 C.F.R. § 164.501.

*Secretary* means the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated. 45 C.F.R. § 160.103.

*Use* means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component (for hybrid entities) that maintains such information. 45 C.F.R. § 160.103.

*Violation or violate* means, as the context may require, failure to comply with an administrative simplification provision.

*Workforce* means employees, volunteers, trainees, or other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity. 45 C.F.R. § 160.103.

## **IV. General Policies and Procedures**

### ***A. Authorization to Use or Disclose Protected Health Information***

#### **1. Policy**

Pepperdine University will obtain an individual's authorization to use or disclose protected health information in accordance with HIPAA and its regulations. Generally, designated covered components do not need to obtain an individual's authorization when using and disclosing protected health information for routine purposes (*e.g.* treatment, payment, or health care operations), or for other limited purposes, as described in Pepperdine University's Notice of Privacy Practices. Otherwise, designated covered components must obtain an individual's valid authorization for the use or disclosure of protected health information.

## 2. Procedure

### Authorization Form

- A Sample Authorization Form is set forth in Section V of this Manual.
- The authorization shall be written in plain language and shall contain the following information:
  - a description of the PHI to be used/disclosed that identifies the information in a specific and meaningful fashion;
  - a description of each purpose of the requested use or disclosure, for example, the statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
  - the name of the person or organization authorized to disclose the PHI;
  - the name of the person or organization authorized to receive the PHI;
  - a statement that the individual has the right to revoke the authorization in writing;
  - a statement listing the exceptions to an individual’s right to revoke;
  - a statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected;
  - a statement that the individual may refuse to sign the authorization;
  - a statement that the covered component will not condition treatment, payment, enrollment or eligibility for benefits in a health plan, based on the individual providing authorization for the requested use or disclosure;
  - an expiration date (or expiration event); and
  - the signature of the individual and date (or the signature of an individual’s personal representative).
- The University must provide the individual with a signed copy of the authorization.

### Psychotherapy Notes

- The University will obtain an individual’s authorization to use or disclose psychotherapy notes, except in the circumstances listed below.
- The University does not need to obtain an individual’s authorization to use or disclose psychotherapy notes:
  - to carry out treatment, payment, or health care operations;
  - for use by the originator of the psychotherapy notes for treatment;
  - for use or disclosure by the designated covered component for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in counseling;
  - for use or disclosure by the covered entity to defend itself in a legal action or proceeding brought by the individual; and
  - for other limited uses and disclosures as described in 45 C.F.R. § 508(a)(2).

### Revocation of Authorization

- An individual may revoke an authorization at any time, provided that the revocation is in writing.
- If the University has already taken action in reliance on the authorization, the University will stop providing the protected health information based on the revoked authorization with a reasonable period of time.

### Documentation

- The University must document and retain any signed authorization under this section.

## **3. Applicable Regulations**

45 C.F.R. §§ 164.508, 164.512.

### ***B. Business Associates***

#### **1. Policy**

From time to time, covered components may share protected health information with external parties, known as business associates. Protected health information generally may only be shared with business associates pursuant to a valid Business Associate Agreement. A Business Associate Agreement can be in the form of a written amendment to an existing agreement.

#### **2. Procedure**

##### Business Associate Agreements

- A Sample Business Associate Agreement is set forth in Section V of this Manual.
- Generally, PHI may only be shared with business associates pursuant to a valid Business Associate Agreement.
- It is the responsibility of each designated covered component contracting with business associates to assure that valid Business Associates Agreements are executed.
- Business Associate Agreements must be in writing and must contain certain language that is HIPAA compliant.

#### **3. Applicable Regulations**

45 C.F.R. §§ 164.502(e), 164.504(e), 164.532, 160.402.

### ***C. Complaint***

#### **1. Policy**

An individual who believes his or her HIPAA privacy rights have been violated may file a complaint regarding the alleged privacy violation with the University's Privacy Official

or the appropriate Office of Civil Rights (OCR) Regional office. Complaints submitted to the University's Privacy Official will be documented, reviewed, and acted upon, if necessary.

## **2. Procedure**

### Filing a Complaint

- A Sample Complaint Form is set forth in Section V of this Manual.
- If an individual believes his or her privacy rights have been violated, an individual may file a complaint with the appropriate OCR Regional office, or with the University's Privacy Official located in the Equal Employment and Opportunity Office, Pepperdine University, 24255 Pacific Coast Highway, Malibu, CA 90263. Each designated covered component must develop and implement a process for receiving complaints and reporting them to the University's Privacy Official (this process can be as simple as instructing individuals who wish to file a complaint to contact the University's Privacy Official).
- Individuals must file complaints in writing, either paper or electronically.
- A complaint must be filed 180 days from when the individual knew or should have known of the circumstance that led to the complaint, unless this time limit is waived for "good cause" shown.
- A complaint must name the entity that is the subject of the complaint and describe the acts or omission believed to be in violation of the HIPAA requirements.
- OCR may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.
- Individuals may not be penalized for filing a complaint.

### Investigation, Sanctions

- The Privacy Official will investigate alleged complaints to determine if a breach of privacy has occurred.
- If the Privacy Official determines that a violation occurred, the Privacy Official will apply appropriate sanctions against the person or entity who failed to comply with the privacy policies and procedures and instruct the person or entity to take the corrective actions, if necessary. The Privacy Official will document any sanctions imposed.

## **3. Applicable Regulations**

45 C.F.R. §§ 160.304, 160.306; 160.308, 160.310, 160.410, 164.530.

### ***D. De-Identification of Protected Health Information***

#### **1. Policy**

The University may use or disclose de-identified PHI without obtaining an individual's authorization. PHI shall be considered de-identified if either of the two de-identification procedures set forth below are followed.

## 2. Procedure

### Removal of Identifiers

- De-identified PHI is rendered anonymous when identifying characteristics are completely removed and when the University does not have any actual knowledge that the information could be used alone or in combination with other information to identify an individual.
- De-identification requires the elimination not only of primary or obvious identifiers, such as the individual's name, address, and date of birth, but also of secondary identifiers through which a user could deduce the individual's identity.
- For information to be de-identified the following identifiers must be removed:
  - Names
  - All address information except for the state
  - Names of relatives and employers
  - All elements of dates (except year), including date of birth, 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
  - Telephone numbers
  - Fax numbers
  - Email addresses
  - Social security number
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers, including license plate numbers
  - Device ID's and serial numbers
  - Web resource locators (URL)
  - Internet protocol (IP) addresses
  - Biometric identifiers
  - Full face photographic images and other comparable images
  - Any other unique identifying number characteristic (except as otherwise permitted for re-identification purposes).

### Statistical Method

- PHI is considered de-identified if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (a) 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 (b) documents the methods and results of the analysis to justify such determination.

### Reidentification

- A covered component 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 component, 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 component 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.

### **3. Applicable Regulations**

45 C.F.R. §§ 164.502(d), 164.514(a) and (b).

#### ***E. Limited Data Sets***

##### **1. Policy**

Covered components may use and disclose a limited data set without an individual's authorization for the purposes of research, public health, or health care operations if the covered component enters into a Data Use Agreement with the intended recipient of the limited data set. A designated covered component may use protected health information to create a limited data set, or to disclose protected health information to a Business Associate to create a limited data set on behalf of the covered component.

##### **2. Procedure**

###### Limited Data Set

- A limited data set is PHI that excludes the following direct identifiers of the individual or relatives, employers, or household members of the individual:
  - Names;
  - Postal address information, other than town, city, state, and zip codes;
  - Telephone numbers;
  - Fax numbers;
  - Electronic mail addresses;
  - Social security numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers (including license plate number);
  - Web Universal Resource Locators (URLs);
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voiceprints; and
  - Full face photographs and comparable images

###### Data Use Agreements. Data Use Agreements must:

- Establish the permitted uses and disclosures of the limited data set;
- Establish who is permitted to use or receive the limited data set; and
- Provide that the recipient of the information will:

- not use or further disclose the information other than as permitted by the agreement;
- use appropriate safeguards to prevent use or disclosure other than as permitted by the agreement;
- report to the University any uses or disclosures the recipient is aware of that is not provided for by the agreement;
- ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient; and
- not identify the information or contact the individuals.

### **3. Applicable Regulation**

45 C.F.R. § 164.514(e).

#### ***F. Minimum Necessary Use and Disclosure of Protected Health Information***

##### **1. Policy**

When using or disclosing PHI or when requesting PHI from another entity covered by the HIPAA privacy regulations, the University shall make a reasonable effort to limit itself to the minimum amount of protected health information necessary to accomplish the intended purpose of the use, disclosure or request. The University is not required to apply the minimum necessary standard under the following circumstances:

- For Treatment. Disclosure to or requests by a health care provider for purposes of diagnosing or treating an individual.
- To the Individual. Uses or disclosures made to the individual.
- Pursuant to Patient's Authorization. Uses or disclosures pursuant to a valid authorization.
- To the HHS. Disclosures to the Office for Civil Rights of the U.S. Department of Health and Human Services for HIPAA compliance purposes.
- Required by Law. Uses or disclosures that are required by law (*i.e.*, a mandate that is contained in law that compels the University to use or disclose protected health information and that is enforceable in a court of law, *e.g.*, court orders, court-ordered subpoenas, civil or authorized investigative demands).

##### **2. Procedure**

The University recognizes that each designated covered component that uses or discloses protected health information has a unique organizational structure and that employees of the unit may perform various functions for the unit that require different levels of access to protected health information. Further, the responsibilities designated to these functions vary across each designated covered component at the University and cannot be determined solely based on job title or description. For these reasons it is the responsibility of each designated covered component that uses and discloses protected health information to determine those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

for each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

For any type of disclosure that it makes on a routine and recurring basis, a covered component must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, the covered component must develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria.

### **3. Applicable Regulations**

45 C.F.R. §§ 164.502 and 164.514(d).

## ***G. Notice of Privacy Practices***

### **1. Policy**

The University will develop and distribute a Notice of Privacy Practices to its designated covered components that includes information required by HIPAA and its regulations. A copy of the Notice of Privacy Practices can also be found at <http://www.pepperdine.edu/provost/Library/HIPAAPractices.pdf>. Designated covered components are encouraged to distribute the Notice of Privacy Practices that the University provides. If a designated covered component elects to develop its own notice or summary of notice, the notice must contain certain information required by law.

### **2. Procedure**

#### Distribution

- Direct Treatment Relationships. Covered components with direct treatment relationships with individuals will provide the Notice of Privacy Practices to each individual no later than the date of the first service delivery after April 14, 2003.
- Indirect Treatment Relationships. Covered components with indirect treatment relationships with individuals will provide the Notice of Privacy Practices upon request.
- Health Plans. A health plan will distribute its Notice to each enrollee by April 14, 2003 and thereafter give its Notice to each new enrollee at enrollment.

#### Availability

- Covered components will make the Notice of Privacy Practices available to any person upon request.
- Covered components will post the Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered component to be able to read it.
- If a covered component develops its own Notice of Privacy Practices, it must post the notice on its website (if it maintains a website).

### Acknowledgement

- Covered components will make a good faith effort to obtain a written acknowledgment from the individual of his or her receipt of the Notice of Privacy Practices.
- If the individual does not acknowledge receipt of the Notice of Privacy Practices, a note should be made indicating why the acknowledgment was not obtained.
- Covered components should not condition treatment or payment on an individual's acknowledgment of the receipt of the Notice of Privacy Practices.
- In emergency situations, the Notice of Privacy Practices may be provided and the acknowledgment obtained at a time reasonably practicable after the emergency treatment situation is resolved.

### Amendments

- If the Notice of Privacy Practices is amended, it will be made available upon request on or after the effective date.
- If the amendment causes a material change to any term of the Notice, the Notice will be distributed in accordance with the distribution procedure above.

- **Applicable Regulation**

45 C.F.R. § 164.520.

## ***H. Privacy Official, Security Official, and Privacy Coordinators***

### **1. Privacy Official**

The University has designated a Privacy Official who is responsible for the development and implementation of the University's policies and procedures related to the privacy and security of protected health information under HIPAA.

Responsibilities of the Privacy Official include:

- Maintain ongoing communication with the Security Official and all Privacy Coordinators.
- Coordinate training programs for the designated covered components in cooperation with the Privacy Coordinators.
- Maintain ongoing communications with the IRB regarding research use of PHI.
- Respond to complaints regarding University policies, procedures and practices related to the privacy of health information.
- Respond to, or refer to the appropriate covered component, requests by individuals for access and amendment, an accounting of disclosures, or requested restrictions to the use and disclosure of the individual's PHI.

The contact information for the Privacy Official is:

Larisa Hamada

15

Last updated on  
7/23/2009

Pepperdine University  
24255 Pacific Coast Highway  
Malibu, CA 90263  
Email: [larisa.hamada@pepperdine.edu](mailto:larisa.hamada@pepperdine.edu)  
Telephone: (310) 506-4208

This information is subject to change and will be revised accordingly.

## **2. Security Official**

The University has designated a Security Official to assist the Privacy Official and Privacy Coordinators in carrying out University adopted policies and procedures related to the privacy and security of individuals' ePHI under HIPAA.

Responsibilities of the Security Official include:

- Maintain ongoing communication with the Privacy Official and all Privacy Coordinators.
- Assist in the development of policies and procedures of each covered component related to the security of ePHI.
- Assist in the development and implementation of ongoing security awareness and training programs for the workforce of covered components, researchers, and students with respect to ePHI.
- Monitor the use of security measures to protect ePHI.
- Monitor the conduct of personnel in relation to ePHI.
- Assist in revising the University's policies and procedures related to the privacy and security of ePHI as required to comply with changes in any applicable laws and document any changes.

The contact information for the Security Official is:

Kim Cary  
Pepperdine University  
24255 Pacific Coast Highway  
Malibu, CA 90263  
Email: [kim.cary@pepperdine.edu](mailto:kim.cary@pepperdine.edu)  
Telephone: (310) 506-6655

## **3. Privacy Coordinators**

The University has designated Privacy Coordinators within each of the covered components to assist the Privacy Official and the Security Officer in carrying out University adopted policies and procedures related to the privacy and security of protected health information under HIPAA.

Responsibilities of the Privacy Coordinators include:

- Perform the role of liaison and maintain ongoing communication with the Privacy Official and the Security Official.
- Communicate with the Privacy Official and the Security Official regarding the privacy and security policies of the covered component within which the Privacy Coordinator is located.
- Develop and maintain procedures consistent with the policy for protection of PHI in the covered component.
- Maintain all policies and procedures in written or electronic form.
- Inform members of the covered component about the policies and procedures through various mechanisms, including staff meetings, orientation for new workforce members, and ongoing education.
- Monitor the process for identifying workforce members within the covered component who require access to PHI.
- Monitor compliance with the policies and procedures of the covered component.
- Report to the Privacy Official violations that result in an impermissible use of disclosure of PHI, and report to the Security Official violations that result in an impermissible use of disclosure of ePHI.
- Help ensure continued compliance with HIPAA and University policies and procedures.

The contact information for each of the Privacy Coordinators is:

Student Health Center  
 Nancy Safinick  
 Email: [nancy.safinick@pepperdine.edu](mailto:nancy.safinick@pepperdine.edu)  
 Telephone: (310) 506-4316  
 (Voicemail Option #3 for Business Inquiries)

Athletic Training Center  
 Kevin Wright, Athletic Trainer  
 Email: [kevin.wright@pepperdine.edu](mailto:kevin.wright@pepperdine.edu)  
 Telephone: (310) 506-4169

Student Counseling  
 Dr. Nivla Fitzpatrick  
 Email: [nivla.fitzpatrick@pepperdine.edu](mailto:nivla.fitzpatrick@pepperdine.edu)  
 Telephone: (310) 506-4210

Pepperdine University Psychological & Educational Clinic  
 West Los Angeles Graduate Campus  
 Dr. Aaron Aviera, Director  
 Email: [aaron.aviera@pepperdine.edu](mailto:aaron.aviera@pepperdine.edu)  
 Telephone: (310)568-5752

Pepperdine Community Counseling Center

Orange County Graduate Campus  
Dr. Duncan Wigg, Director  
Email: [Duncan.wigg@pepperdine.edu](mailto:Duncan.wigg@pepperdine.edu)  
Telephone: (949) 223-2522

Pepperdine Community Counseling Center  
Encino Graduate Campus  
Dr. Anat Cohen, Director  
Email: [anat.cohen@pepperdine.edu](mailto:anat.cohen@pepperdine.edu)  
Telephone: (818) 501-1660

Pepperdine Jerry B.H. Union Rescue Clinic  
Dr Aaron Aviera, Director  
Pepperdine University Psychology & Educational Clinic  
Email: [aaron.aviera@pepperdine.edu](mailto:aaron.aviera@pepperdine.edu)  
Telephone: (310) 568-5752

Center for Human Resources  
Angie Pedersen  
Email: [angie.pedersen@pepperdine.edu](mailto:angie.pedersen@pepperdine.edu)  
Telephone: (310)506-4190

This contact information is subject to change and will be revised accordingly.

## **1. Applicable Regulation**

45 C.F.R. § 164.530(a).

### ***1. Records Retention***

#### **1. Policy**

The University will maintain certain documentation regarding its HIPAA compliance, in written or electronic form.

#### **2. Procedure**

- Covered components must retain the following documentation for six years from the date of its creation or the date it was last in effect (whichever is later):
  - Policies and Procedures. Any policy or procedural documentation, including notice of privacy practices, consents (if any) and authorizations, and other standard forms.
  - Patient Requests. Patient requests for access, amendment, or accounting of disclosures.
  - Complaints. The handling of any individual's complaints.
  - Workforce Training. The processes for and content of workforce training.

- Sanctions. The handling of any sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered component.
- If state laws require longer retention periods, the state requirements control.

### **3. Applicable Regulation**

45 C.F.R. § 164.530(j).

## ***J. Research***

### **1. Policy**

HIPAA establishes privacy protections for human subjects research and establishes the conditions under which protected health information may be used or disclosed by Pepperdine University for research purposes. This policy and procedure should be followed in addition to any applicable federal or state regulations governing the protection of human subjects research, as well as any applicable Institutional Review Board (“IRB”) policies and procedures.

### **2. Procedure**

#### Research

- Pepperdine University may use or disclose protected health information for research, regardless of the source of the funding of the research, in the following circumstances:
  - Individual Authorization. The individual has signed a valid authorization;
  - Board Approval of Waiver. The IRB has approved a proper waiver of the need to obtain the individual’s authorization;
  - Limited Data Set. The health information is used or disclosed in a limited data set in accordance with a valid Data Use Agreement;
  - De-identification. The health information has been de-identified;
  - Preparatory to Research. PHI may be used or disclosed to a researcher as necessary to prepare a research protocol or for similar purposes preparatory to research if the University obtains the following representations from the researcher: (a) the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; (b) no PHI will be removed from the University by the researcher in the course of the review; and (c) the PHI for which use or access is sought is necessary for the research purposes;
  - Decedent’s Research. PHI may be used or disclosed to a researcher for research on decedents if the University obtains the following from the researcher: (a) a representation that the use or disclosure sought is solely for research on the PHI of decedents; (b) documentation of the death of such individual(s) and/or research subject(s); (c) a representation that the PHI for which use or disclosure is sought is necessary for research purposes.
- If the University is also the researcher, the University must still obtain the proper authorization or fit within one of the other exceptions before using PHI for research purposes.

#### Research Pursuant to an Authorization

- Research authorizations must contain the same core elements as other authorizations (see Section IV. A.), except for the following differences:
  - The University may condition the provision of research-related treatment on a provision of authorization for the use or disclosure of protected health information for such research;
  - An authorization for use and disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;
  - A research authorization does not need to contain an expiration date or event as is required for other authorizations (the language “end of the research study” or “none” or similar language is sufficient).

#### Revocation

- A research authorization may be revoked by an individual.
- If an authorization is revoked, the University may continue its use or disclosure of the PHI already obtained pursuant to the valid authorization to the extent necessary to preserve the integrity of the research study.

#### IRB Waiver Approval

- For a use or disclosure to be permitted upon IRB approval, the IRB must document that all of the following criteria have been met:
  - The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on the presence of the following elements: (i) an adequate plan to protect the identifiers from improper use and disclosure; (ii) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (iii) adequate written assurances that the protected health information 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 protected health information would be permitted under this policy;
  - The research could not be conducted without the waiver or alteration; and
  - The research could not be conducted without access to and use of the protected health information.
- The documentation should include a statement identifying the IRB and the date on which the alteration or waiver of authorization was approved.
- The documentation should include a brief description of the PHI for which use or access has been determined to be necessary by the IRB.
- The documentation should include a statement that the alteration or waiver of authorization has been reviewed.
- The Chair of the IRB or other member designated by the Chair must sign the document.

### **3. Applicable Regulations**

45 C.F.R. §§ 164.501, 508, 512.

#### ***K. Right to Request Access to Protected Health Information***

##### **1. Policy**

Individuals have the right to request access to inspect or copy their protected health information that is maintained in a designated record set. The University will address an individual's request to inspect or copy his or her protected health information in a timely and professional manner. Individuals do not have the right to access certain types of information (set forth below), and in those situations, the University may deny an individual's request to access. In certain circumstances, an individual may have the right to have a denial reviewed. The University will adhere to the procedures set forth below when addressing, denying, or reviewing an individual's request to access.

##### **2. Procedure**

###### Requests for Access

- A Sample Request for Access Form is set forth in Section V of this Manual.
- Each covered component must designate the title of the person(s) or office responsible for receiving and processing requests for access by individuals.
- Individuals must be instructed to direct their request for access to the designated person responsible for receiving such requests.
- Individuals may be instructed to make their request for access in writing.
- The person responsible for processing the request may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate a timely provision of access.
- The parties can agree in advance that a summary of the requested protected health information will be provided in lieu of access to the information.
- Upon receipt of a proper request, the covered component will act on the request by either: (1) informing the individual of acceptance and providing the access requested; or (2) providing the individual with a written denial in accordance with the procedure set forth below.
- If the covered component does not maintain the requested protected health information, but it knows where the requested information is maintained, the covered component will inform the individual where to direct the request for access.
- An individual's request for access must be acted upon no later than 30 days after the request is made; or, if the request is for protected health information that is not maintained or accessible on-site, no later than 60 days after the request.

###### Providing Access

- If a request for access is granted, the individual will be given access to the protected health information in a secure and confidential manner.
- The covered component will provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format. If it is not readily producible in such

- format, the covered component will provide the access in such other form as agreed to by the individual.
- In instances where the protected health information is in more than one record set, or at more than one location, the covered component will only produce the protected health information once in response to the request for access.

### Denial of Access

- A Sample Denial of Access Form is set forth in Section V of this Manual.
- A written denial of access may be issued in the following circumstances:
  - Psychotherapy Notes. An individual does not have the right to access psychotherapy notes relating to him or herself except (a) to the extent the patient's treating professional approves to such access in writing; or (b) the patient obtains a court order authorizing such access.
  - Legal Information. An individual does not have the right to access information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
  - Endangerment. An individual does not have the right to access information in the event that a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
  - Obtained from Someone Else. An individual does not have the right to access information if the protected health information 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.
  - Reference to Other People. An individual does not have the right to access information if the protected health information makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
  - Personal Representative. An individual does not have the right to access information if the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
  - Research. The University may temporarily suspend an individual's access to protected health information created or obtained in the course of research that includes treatment. The suspension may last for as long as the research is in progress, provided that the individual agreed to the denial of access when consenting to participate in the research, and the individual has been informed that the right of access will be reinstated upon completion of the research.

- Other Limited Circumstances. There are other limited circumstances when an individual does not have the right to access protected health information, listed in 45 C.F.R. § 164.524.
- When denying an individual access to protected health information, the denial will be written in plain language and
  - Contain the basis for the denial;
  - If applicable, contain a statement of the individual's review rights, including a description of how the individual may exercise such rights; and
  - Contain a description of how the individual may complain to the University pursuant to the University's complaint process (and include the title and telephone number of the contact person), or to the appropriate OCR Regional office.
- The University must, to the extent possible, grant the individual access to any other protected health information requested after excluding the protected health information that was denied.

#### Reviewing a Denial of Access

- If access is denied based on (1) Endangerment; (2) Reference to Other People; or (3) Personal Representative (these exceptions are all set forth above), the individual must be given the opportunity to have the denial reviewed.
- If an individual has requested a review of denial, the University must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access.
- The reviewing official must determine whether or not to confirm the denial based on the standards set forth in 45 C.F.R. 164.524(a)(3). The reviewing official must review the denial of access within a reasonable period of time and then must promptly notify the individual of the decision and take any necessary action to carry out the reviewing official's decision.

#### Costs and Fees

- The University may impose a reasonable, cost-based fee for copying costs and postage in response to a request for access.
- If the individual agrees in advance, the University may impose a reasonable cost-based fee for preparing a summary of the protected health information.

#### Documentation

- The University must document and retain:
  - the designated record sets that are subject to access by individuals; and
  - the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

### **3. Applicable Regulation**

45 C.F.R. § 164.524.

## ***L. Right to Request an Accounting of Disclosures***

### **1. Policy**

The University will permit individuals to request and receive an accounting of disclosures of their protected health information. An individual may request an accounting for disclosures that have been made up to six years prior to the date of his or her request; however, the University is not required to account for any disclosures that occurred prior to the HIPAA compliance date of April 14, 2003. The accounting must include all disclosures except for the following:

- Disclosures made to carry out treatment, payment, or health care operations;
- Disclosures made to the individual;
- Disclosures made pursuant to an individual's authorization;
- Disclosures for a facility directory;
- Disclosures to persons directly involved in the individual's care or payment or disclosures for notification purposes pursuant to 45 C.F.R. § 164.510(b);
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional facilities or law enforcement officials;
- Disclosures made as part of a limited data set;
- Disclosures that occurred prior to the compliance date; and
- Other limited disclosures as set forth in 45 CFR § 164.528.

### **2. Procedure**

#### Request for Accounting

- Individuals will be permitted to request and receive an accounting of disclosures of their protected health information.
- Designated covered components may require requests for an accounting to be submitted in writing.
- A Sample Request for Accounting of Disclosures Form is set forth in Section V of this Manual.

#### Accounting Requirements

- A Sample Accounting for Disclosures Form is set forth in Section V of this Manual.
- An individual must receive a written accounting of disclosures and the written accounting must include:
  - the date of disclosure;
  - the name of the entity or person who received the protected health information and, if known, the address of such entity or person;
  - a brief description of the protected health information disclosed; and
  - a brief statement of the purpose of the disclosure; or in lieu of such statement, a copy of a written request for a disclosure, if any.
- If the University has made multiple disclosures of the protected health information to the same person or entity for a single purpose, or pursuant to a single authorization, the accounting may, with respect to such multiple disclosures, provide:

- the information required above for the first disclosure during the accounting period;
  - the frequency or number of disclosures made during the accounting period; and
  - the date of the last such disclosure during the accounting period.
- The University must act on the individual's request for an accounting no later than 60 days after receipt of such a request. If the University is unable to provide the accounting within this time frame, it may extend the time to provide the accounting by no more than 30 days, provided that: (1) the University provides the individual with a written statement of the reasons for the delay and the date by which the University will provide the accounting; and (2) the University may have only one such extension of time for action on a request for an accounting.

#### Suspension of Accounting of Disclosures

- An accounting of disclosures may be suspended at the request of a health oversight agency or law enforcement official if certain conditions are met.
- If a designated health care component receives a request to suspend an individual's right to receive an accounting of disclosures, the designated covered component should contact the University's Privacy Official.

#### Costs and Fees

- The first accounting of disclosures to an individual in any twelve (12) month period must be provided at no charge.
- A reasonable cost-based fee may be imposed for each subsequent request for an accounting by the same individual within the 12-month period, provided that the University informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request.

### **3. Applicable Regulation**

45 C.F.R. § 164.528.

#### ***M. Right to Request an Amendment to Protected Health Information***

##### **1. Policy**

Individuals have the right to request an amendment or correction to their protected health information. The University will permit an individual to request an amendment to his or her protected health information in their designated record set for as long as the information is maintained in the designated record set. An individual can request an amendment to his or her protected health information that was not created by the University, but the individual must provide the University with a reasonable basis to believe that the originator of the information is no longer available to act on the request. The University has the right to deny the request to amend in certain circumstances.

## 2. Procedure

### Requests for an Amendment

- A Sample Request for an Amendment Form is set forth in Section V of this Manual.
- Each covered component of the University must designate the title of the person(s) or office responsible for receiving and processing request for an amendment by individuals.
- Individuals must be instructed to direct their requests for an amendment to the designated person responsible for receiving such request.
- A covered component may instruct individuals to make their requests in writing and may require the individual to provide a reason to support the requested amendment, as long the designated covered component informs the individual in advance of such requirements.
- The University must act upon an individual's request for amendment no later than 60 days after receipt of the request. If the covered entity is unable to act on the amendment within this time period, the University may extend the time for such action by no more than 30 days, provided that: (1) the University provides the individual with a written statement of the reasons for the delay and the date by which the University will complete its action on the request; and (2) the University may have only one such extension of time for action on a request for an amendment.

### Accepting a Request to Amend

- If the requested amendment is accepted, in whole or in part, the covered component shall inform the individual of the acceptance and make the appropriate amendment.
- At a minimum, the covered component shall amend the information by identifying the affected information in the designated records set and appending or otherwise providing a link to the location of the amendment.
- The covered component and the individual should identify the relevant persons or entities, including business associates, who need to be informed about the amendment.

### Denying a Request to Amend

- A Sample Denial of Request for an Amendment Form is set forth in Section V of this Manual.
- An individual's request for an amendment may be denied if the covered component determines that the protected health information or record that is the subject of the request:
  - was not created by the University, unless the individual provides a reasonable basis to believe that the originator of the protected health information is not longer available to act on the requested amendment;
  - is not part of the individual's designated record set;
  - is not available for inspection by the individual pursuant to the Access to Right to Request Access to PHI policy, set forth herein; and
  - is accurate and complete.

- If a covered component denies the requested amendment, the covered component shall inform the individual in writing.
- The denial shall be written in plain language and contain the following:
  - The basis for the denial;
  - A statement notifying the individual that he or she has the right to submit a written statement of disagreement and a description of how the individual may file such a statement;
  - A statement notifying the individual that if he or she does not submit a statement of disagreement, the individual may request that the designated covered component provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and
  - A description of how the individual may file a complaint pursuant to the Privacy Complaint Policy and Procedure, set forth above.
- If the University denies a request for an amendment, the individual has the right to file a statement of disagreement.

#### Statement of Disagreement

- If the University denies an individual's request for an amendment, the individual will have the right to submit a statement of disagreement.
- The University may then prepare a written rebuttal to the individual's statement of disagreement.
- A copy of the rebuttal must be provided to the individual.

### **3. Applicable Regulation**

45 C.F.R. § 164.526.

## ***N. Right to Request Confidential Communications***

### **1. Policy**

Individuals may request to receive communications of protected health information in a confidential manner (e.g., by alternative means or in alternative locations). The University shall accommodate reasonable requests to receive confidential communications.

### **2. Procedure**

- A covered component may require an individual to make a request to receive confidential communications in writing.
- Covered components may condition the provision of a reasonable accommodation on: (1) information as to how payment (if any) will be handled; and (2) specification of an alternative address or other method of contact.
- A covered component may not require an explanation from the individual as to the basis for the request as a condition of providing confidential communications.

### **3. Applicable Regulation**

45 C.F.R. § 164.522(b).

#### ***O. Right to Request Restrictions on the Use and Disclosure of Protected Health Information***

##### **1. Policy**

Individuals may request restrictions on the use and disclosure of their protected health information. Requests for restriction do not have to be granted; however, if the University agrees to a restriction, it may not use or disclose the protected health information in violation of the restriction, except in emergency situations. Further, any agreed-to restriction will not be effective to prevent uses and disclosures to the individual or as required by law.

##### **2. Procedure**

###### Request to Restrict Use or Disclosure of Protected Health Information

- An individual may request a restriction on the use and disclosure of his or her protected health information.
- A covered component does not have to agree to requests for restrictions; however, if it does agree, the covered component may not use or disclose the protected health information in violation of such restriction, except in emergency situations.
- The covered component should discuss with the individual whether the restriction should be communicated to others (i.e., other covered components of the University or business associates who may be sending the individual communications on behalf of the University).

###### Terminating a Restriction

- A restriction can be terminated if:
  - the individual requests the restriction in writing or orally (if the termination is requested orally, it should be documented); or
  - The designated covered component informs the individual that it is terminating the agreement to a restriction, in which case the termination will only apply to protected health information created or received after the individual has been notified of the termination.

### **3. Applicable Regulation**

45 C.F.R. § 164.522(a).

#### ***P. Safeguarding Protected Health Information***

##### **1. Policy**

Pepperdine University will implement appropriate administrative, technical, and physical safeguards which will reasonably safeguard the confidentiality of protected health

information. Designated covered components may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the privacy of protected health information in light of the unique circumstances of a particular component.

## **2. Procedure**

The University recognizes that each designated covered component has a unique organizational structure. For this reason, it is the responsibility of each designated covered component to determine and implement reasonable administrative, technical, and physical safeguards. The following list of guidelines contains some suggestions of administrative, technical, and physical safeguards that covered components may wish to adopt:

- Oral Communications. Exercising due care to avoid unnecessary disclosures of protected health information through oral communications, such as avoiding such conversations in public areas.
- Telephone Messages. Limiting messages left on answering machines and voicemails to appointment reminders and messages that do not link an individual's name to protected health information.
- Faxes. Placing fax machines in secure areas not readily accessible to visitors, clients, patients, etc. and/or using a cover sheet with a confidentiality notice when faxing protected health information.
- Paper Records. Storing paper records and charts in a way that avoids access by unauthorized persons, such as in locked filing cabinets.
- Desks and Working Areas. Securing desks and working areas that contain protected health information.
- Computer Monitors. Positioning computer monitors away from common areas or installing a privacy screen to prevent unauthorized viewing, and/or creating password protected screen savers.
- Disposal of Paper Records. Disposing of documents containing protected health information in a secure manner, e.g., by shredding.
- Disposal of Electronic Materials. Disposing of electronic material that contains unencrypted protected health information in a secure method.
- E-mails. Sending e-mails that contain protected health information with a confidentiality notice, and/or sending such e-mails in encrypted form.
- Electronic Documents. Securing protected health information that is stored on a hard disk drive or other internal component of a personal computer, such as by password or encryption.

## **3. Applicable Regulation**

45 C.F.R. § 164.530(c).

### ***Q. Training***

#### **1. Policy**

Each designated covered component is responsible for training its workforce (including employees, students, volunteers, etc.) with respect to the University's HIPAA policies

and procedures on the use and disclosure of PHI as necessary and appropriate for the members of the workforce to carry out their function.

## **2. Procedure**

### Training

- It will be the responsibility of each designated covered component to ensure that its workforce receives training.
- Each employee must be trained no later than the April 14, 2003. Each new employee must receive training within a reasonable period of time after the person becomes an employee, etc.
- If there is a material change in the policies and procedures and, as a result, certain employees are affected, those employees must receive training on the material change within a reasonable period of time after the change becomes effective.

### Documentation

- A covered entity must document that the training has been provided.

## **3. Applicable Regulation**

45 CFR § 164.530(b).

## **V. HIPAA Sample Forms [see following pages]**

*A. Accounting for Disclosures of Protected Health Information*

*B. Authorization to Use/Disclose Protected Health Information*

*C. Business Associate Agreement*

*D. Denial of Request for Amendment*

*E. Denial of Request for Access*

*F. Privacy Complaint*

*G. Request for Access to Protected Health Information*

*H. Request for Accounting of Disclosures*

*I. Request for Amendment to Protected Health Information*



**Pepperdine University**  
**Authorization to Use/Disclose Protected Health Information (HIPAA)**

Name: \_\_\_\_\_

Location: \_\_\_\_\_ Telephone Number: \_\_\_\_\_

I hereby authorize the use and/or disclosure of my health information as described below. I understand that this authorization is voluntary. I also understand that if the person or organization authorized to receive the information is not a health plan or health care provider, the released information may be redisclosed and may no longer be protected by the federal privacy regulations.

1. Person or organization authorized to disclose the health information:  
\_\_\_\_\_

2. Person or organization authorized to receive the health information:  
\_\_\_\_\_

3. Description of health information that may be used/disclosed:  
\_\_\_\_\_

4. Description of each purpose for which the health information will be used/disclosed (*Note: Not required if disclosure is requested by the individual*):  
\_\_\_\_\_

5. I understand that the person or organization that I am authorizing to use/disclose the information may receive compensation in exchange for the health information described above.

6. I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to enroll in a health plan, obtain health care treatment or payment or my eligibility for benefits.\* (*Note: Not required if disclosure is requested by the individual.*)

7. I understand that I may revoke this authorization at any time by providing written notice to:

\_\_\_\_\_  
I understand that my revocation will not affect any actions already taken in reliance on this authorization.

8. I understand I may inspect or copy any information to be used or disclosed under this authorization.

9. Unless otherwise revoked in writing, this authorization will expire \_\_\_\_\_ days from the date signed below. If this date is left blank, the authorization will automatically expire one year from the date I sign below.

\_\_\_\_\_  
Signature of Individual (or Legal Representative)

\_\_\_\_\_  
Date

\_\_\_\_\_  
(Print) Individual's Name

\_\_\_\_\_  
(Print) Name of Legal Representative (if applicable)

\_\_\_\_\_  
Relationship to Individual

\* A health plan may condition enrollment or eligibility for benefits on an individual providing an authorization prior to enrollment if the authorization sought is for the plan's eligibility or enrollment determinations relating to the individual or for its underwriting risk or risk rating determinations and the authorization is not for a use or disclosure of psychotherapy notes (45 CFR §164.508(b)(4)(ii)(A&B)).

## Pepperdine University Business Associate Agreement

**[This is a sample Business Associate Agreement. Words or phrases contained in brackets are intended as either optional language or as instruction to the users and are not intended to be included in the contractual provisions.]**

This Agreement is made on **[date]**, by and between Pepperdine University, **[name of department / covered component]**, 24255 Pacific Coast Highway, Malibu, California 90263 (“COVERED ENTITY”) and **[name of business associate]** (“BUSINESS ASSOCIATE”). This Agreement serves as an addendum to **[reference underlying agreement]**, which is incorporated herein by reference.

### WITNESSETH

WHEREAS, COVERED ENTITY has established a need for certain professional services; and

WHEREAS BUSINESS ASSOCIATE has proposed to provide professional services for COVERED ENTITY;

NOW THEREFORE, in consideration of the mutual covenants and agreements stated herein and of the payments for services hereinafter described, the parties hereto do mutually agree as follows:

1. Employment of BUSINESS ASSOCIATE. COVERED ENTITY hereby agrees to engage BUSINESS ASSOCIATE and BUSINESS ASSOCIATE agrees to perform services hereinafter set forth.
2. Time of Performance. This Agreement and all rights and duties created hereunder will commence \_\_\_\_\_ and terminate \_\_\_\_\_, unless earlier terminated as provided in this Agreement or **[reference underlying agreement]**.
3. Scope of Service and Payment. BUSINESS ASSOCIATE agrees to provide services and COVERED ENTITY agrees to provide payment as specified in detail in **[reference underlying agreement]**.
4. Contacts for Responsibility. The designated representative of COVERED ENTITY for purposes of administering this Agreement shall be \_\_\_\_\_.

The designated representative of BUSINESS ASSOCIATE for purposes of administering this Agreement shall be: \_\_\_\_\_.

### Specific Definitions

5. Catch-all Definition. Terms used, but not otherwise defined in this Agreement shall have the same meaning as those terms in the Privacy Rule.
6. BUSINESS ASSOCIATE shall mean \_\_\_\_\_.
7. COVERED ENTITY shall mean Pepperdine University, [**name of department / covered component**].
8. Individual. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
9. Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
10. Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 164.501, limited to the information created or received by BUSINESS ASSOCIATE from or on behalf of COVERED ENTITY.
11. Required By Law. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.501.
12. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

### Obligations and Activities of Business Associate

13. BUSINESS ASSOCIATE agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
14. BUSINESS ASSOCIATE agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
15. BUSINESS ASSOCIATE agrees to mitigate, to the extent practicable, any harmful effect that is known to BUSINESS ASSOCIATE of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
16. BUSINESS ASSOCIATE agrees to report to COVERED ENTITY any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

17. BUSINESS ASSOCIATE agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by BUSINESS ASSOCIATE on behalf of COVERED ENTITY agrees to the same restrictions and conditions that apply through this Agreement to BUSINESS ASSOCIATE with respect to such information.
18. BUSINESS ASSOCIATE agrees to provide access, at the request of COVERED ENTITY, and in a reasonable time and manner, to Protected Health Information in a designated record set, to COVERED ENTITY or, as directed by COVERED ENTITY, to an Individual in order to meet the requirements under 45 CFR § 164.524.
19. BUSINESS ASSOCIATE agrees to make any amendment(s) to Protected Health Information in a designated record set that the COVERED ENTITY directs or agrees to pursuant to 45 CFR § 164.526 at the request of COVERED ENTITY or an Individual, and in a reasonable time and manner.
20. BUSINESS ASSOCIATE agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by BUSINESS ASSOCIATE on behalf of, COVERED ENTITY available to COVERED ENTITY or to the Secretary, in a reasonable time and manner or designated by the Secretary, for purposes of the Secretary determining COVERED ENTITY'S compliance with the Privacy Rule.
21. BUSINESS ASSOCIATE agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for COVERED ENTITY to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR§ 164.528.
22. BUSINESS ASSOCIATE agrees to provide to COVERED ENTITY or an Individual, in a reasonable time and manner, information collected in accordance with Section 21 of this Agreement, to permit COVERED ENTITY to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

### **Permitted Use and Disclosures by Business Associate**

#### **General Use and Disclosure Provisions**

23. Except as otherwise limited in this Agreement, BUSINESS ASSOCIATE may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, COVERED ENTITY as specified in [**reference underlying agreement**], provided that such use or disclosure would not violate the Privacy

Rule if done by COVERED ENTITY or the minimum necessary policies and procedures of the COVERED ENTITY.

### **Specific Use and Disclosure provisions**

**[Note: THESE ARE OPTIONAL PROVISIONS AND MAY NOT BE APPLICABLE UNDER THIS AGREEMENT]**

24. Except as otherwise limited in this Agreement, BUSINESS ASSOCIATE may use Protected Health Information for the proper management and administration of the BUSINESS ASSOCIATE or to carry out the legal responsibilities of the BUSINESS ASSOCIATE.
25. Except as otherwise limited in this Agreement, BUSINESS ASSOCIATE may disclose Protected Health Information for the proper management and administration of the BUSINESS ASSOCIATE provided that disclosures are Required By Law, or BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.
26. Except as otherwise provided in this Agreement, BUSINESS ASSOCIATE may use Protected Health Information to provide data aggregation services to COVERED ENTITY as permitted by 45 CFR § 164.504(e)(2)(i)(B).
27. BUSINESS ASSOCIATE may use Protected Health Information to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j)(1).

### **Obligations of Covered Entity**

#### **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

28. COVERED ENTITY shall notify BUSINESS ASSOCIATE of any limitation(s) in its notice of privacy practices of COVERED ENTITY in accordance with 45 CFR § 164.520, to the extent that such limitation may affect BUSINESS ASSOCIATE'S use or disclosure of Protected Health Information.
29. COVERED ENTITY shall notify BUSINESS ASSOCIATE of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect BUSINESS ASSOCIATE'S use or disclosure of Protected Health Information.

30. COVERED ENTITY shall notify BUSINESS ASSOCIATE of any restriction to the use or disclosure of Protected Health Information that COVERED ENTITY has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect BUSINESS ASSOCIATE'S use or disclosure of Protected Health Information.

### **Permissible Requests by Covered Entity**

31. COVERED ENTITY shall not request BUSINESS ASSOCIATE to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by a COVERED ENTITY. **[Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of the Business Associate]**

### **Miscellaneous Provisions**

32. Nonassignability. This Agreement shall not be assigned by BUSINESS ASSOCIATE and any attempt to do so shall be void and have no effect.
33. Survival. The respective rights and obligation of BUSINESS ASSOCIATE under Section 39 of this Agreement shall survive the termination of this Agreement.
34. Amendments. This Agreement may be amended at any time by mutual written agreement of the parties hereto.
35. Interpretation. Any ambiguity in this Agreement shall be resolved to permit COVERED ENTITY to comply with the Privacy Rule.
36. Applicable Law. This Agreement shall be governed by California law.

### **Term and Termination**

37. Term. The Term of this Agreement shall be effective as of \_\_\_\_\_, and shall terminate when all of the Protected Health Information provided by COVERED ENTITY to BUSINESS ASSOCIATE, or created or received by BUSINESS ASSOCIATE on behalf of COVERED ENTITY, is destroyed or returned to COVERED ENTITY, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
38. Termination for Cause. Upon COVERED ENTITY'S knowledge of a material breach by BUSINESS ASSOCIATE, COVERED ENTITY shall either:

- a. Provide an opportunity for BUSINESS ASSOCIATE to cure the breach or end the violation and terminate this Agreement [**and the underlying agreement / sections of the underlying agreement**] if BUSINESS ASSOCIATE does not cure the breach or end the violation within the time specified by COVERED ENTITY;
  - b. Immediately terminate this Agreement [**and the underlying agreement / sections of the underlying agreement**] if BUSINESS ASSOCIATE has breached a material term of this Agreement and cure is not possible; or
  - c. If neither termination nor cure is feasible, COVERED ENTITY shall report the violation to the Secretary.
39. Effect of Termination. Upon termination of this Agreement for any reason, BUSINESS ASSOCIATE shall return or destroy all Protected Health Information received from COVERED ENTITY, or created or received by the BUSINESS ASSOCIATE on behalf of the COVERED ENTITY. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall retain no copies of the Protected Health Information.

In the event that BUSINESS ASSOCIATE determines that returning or destroying the Protected Health Information is infeasible, BUSINESS ASSOCIATE shall provide to COVERED ENTITY notification of the conditions that make return or destruction infeasible. Upon [**insert negotiated terms**] that return or destruction of Protected Health Information is infeasible, BUSINESS ASSOCIATE shall extend the protections of this Agreement to such Protected Health Information and shall limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as the BUSINESS ASSOCIATE maintains such Protected Health Information.

IN WITNESS WHEREOF, COVERED ENTITY and BUSINESS ASSOCIATE have executed this Agreement as of the date first written above.

ATTEST:

by \_\_\_\_\_  
PEPPERDINE UNIVERSITY

Date \_\_\_\_\_

ATTEST:

by \_\_\_\_\_

Date \_\_\_\_\_

**Pepperdine University**  
**Denial of Request for an Amendment**

To: \_\_\_\_\_  
*[name of individual]*

Your request to amend your Protected Health Information to Pepperdine University has been denied because (state basis for denial):

---

---

---

\_\_\_\_\_  
(Print) Responsible Party's Name (title of the persons or offices responsible for receiving and processing the request)

\_\_\_\_\_  
Date

You may have the right to submit a written statement of disagreement. If you have the right to submit a written statement of disagreement, submit it to:

\_\_\_\_\_  
*[name of department]*

If you do not submit a written statement disagreeing with the denial, you may request, in writing, that we provide your request for amendment and our denial with any future disclosures of the Protected Health Information that is the subject of your request.

You may make a complaint to the University's Privacy Official regarding the denial of your amendment. The contact information for Privacy Official is:

Larisa Hamada  
Pepperdine University  
24255 Pacific Coast Highway  
Telephone: (310) 506-4208  
E-Mail: [larisa.hamada@pepperdine.edu](mailto:larisa.hamada@pepperdine.edu)

You also may submit a written complaint to the appropriate Office of Civil Rights Regional Office.

**Pepperdine University**  
**Denial of Request for Access**

Your request to access or obtain a copy of your Protected Health Information has been denied for the following reasons:

---

---

---

\_\_\_\_\_  
(Print) Responsible Party's Name (title of the persons or offices responsible for receiving and processing the request)

\_\_\_\_\_  
Date

In accordance with applicable law and Pepperdine University's HIPAA privacy policies, you \_\_\_\_ do \_\_\_\_ do not (*please check one*) have the right to have this denial reviewed by Pepperdine.

If this denial is subject to review as indicated above and you desire to have the decision reviewed, please check the box below and return this form within 30 calendar days to:

\_\_\_\_\_  
*[name of department and address]*

If you desire to register a complaint regarding this denial, you may file a complaint with Pepperdine University's HIPAA Privacy Official or with the appropriate Office of Civil Rights Regional Office

To file a complaint with the University's Privacy Official, contact Larisa Hamada at 24425 Pacific Coast Highway, Malibu, California 90263, (310)-506-\_\_\_\_ or [larisa.hamada@pepperdine.edu](mailto:larisa.hamada@pepperdine.edu).

\* \* \* \* \*

I hereby request a review of Pepperdine University's denial of my request to access or obtain a copy of my Protected Health Information.

\_\_\_\_\_  
Signature of Individual or Legal Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Name of Individual or Legal Representative

**Pepperdine University  
Privacy Complaint**

Name: \_\_\_\_\_ Date: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_

Please describe the nature of the complaint: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Date of Occurrence: \_\_\_\_\_ Information Affected: \_\_\_\_\_

Please name the entity that is the subject of the complaint: \_\_\_\_\_

\_\_\_\_\_  
Signature Date

---

Please mail this form to the University's Privacy Official at the following address:

Larisa Hamada  
HIPAA Privacy Official  
24255 Pacific Coast Highway  
Malibu, California 90263

You may also submit the complaint electronically to [larisa.hamada@pepperdine.edu](mailto:larisa.hamada@pepperdine.edu). A complaint must be filed within 180 days of when you knew or should have known of the circumstances that led to the complaint.

You also may submit a written complaint to the appropriate Office of Civil Rights Regional Office.

**Pepperdine University  
Request for Access to Protected Health Information**

I understand that I have the right to inspect or receive a copy of my Protected Health Information. I understand that the University may impose a reasonable cost-based fee for copying and postage. I further understand that the University may impose a reasonable cost-based fee for preparing a summary of the Protected Health Information if the parties agreed to such summary and fees in advance. I understand that my request to access or inspect my records may be subject to some legal limitations.

**Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**Telephone Number:** \_\_\_\_\_

I hereby request access of the Protected Health Information in my designated record set from \_\_\_\_\_ to \_\_\_\_\_ maintained or created by Pepperdine University, \_\_\_\_\_ (name of department).

1. Identify the records you wish to inspect.

\_\_\_\_\_  
\_\_\_\_\_

2. Please state how you would like to inspect or review your records. For example, do you want to inspect them during regular business hours at Pepperdine University, or do you want copies mailed to you, or do you want to pick up copies at a time and place designated by Pepperdine, etc.

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Signature of Individual (or Legal Representative)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Individual's Name

\_\_\_\_\_  
(Print) Name of Legal Representative (if applicable)

\_\_\_\_\_  
Relationship to Individual

-----  
(For office use only)

\_\_\_ Request Denied \_\_\_ Approved as Requested \_\_\_ Approved per Comments

Comments: \_\_\_\_\_

Responsible Party: \_\_\_\_\_

Date: \_\_\_\_\_

If the request for access is denied, the individual must be informed in writing.



**Pepperdine University**  
**Request for Amendment to Protected Health Information**

Name: \_\_\_\_\_ Date: \_\_\_\_\_  
Telephone Number: \_\_\_\_\_

I hereby request that Pepperdine University \_\_\_\_\_, amend:  
*(name of department)*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Please identify the relevant persons or entities who need to be informed about the amendment: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Please state the reason(s) supporting the requested amendment:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
Signature of Individual (or Legal Representative)

\_\_\_\_\_  
Date

\_\_\_\_\_  
(Print) Individual's Name

\_\_\_\_\_  
(Print) Name of Legal Representative (if applicable)

\_\_\_\_\_  
Relationship to Individual

\_\_\_\_\_  
(Print) Responsible Party's Name (title of the persons or offices responsible for receiving and processing the request)

\_\_\_\_\_  
Date