Trường Đại học Bách Khoa
TPHCM - ĐHQG TPHCM

MINI PROJECT

LAWS, POLICIES, AND STANDARDS IN CYBER-SECURITY

HIPAA

Đinh Thanh Phong - 2270243
Trần Hoàng Nguyên - 2270012
Phạm Đăng Khoa - 2171053

Tổng quan lý thuyết

HIPAA

Introduction to HIPAA for Health Care Professionals

Gerald P. Koocher, Ph.D., ABPP

Content

I. The Importance of Protecting Patient Health Information

II. General HIPAA and Privacy Rule Overview

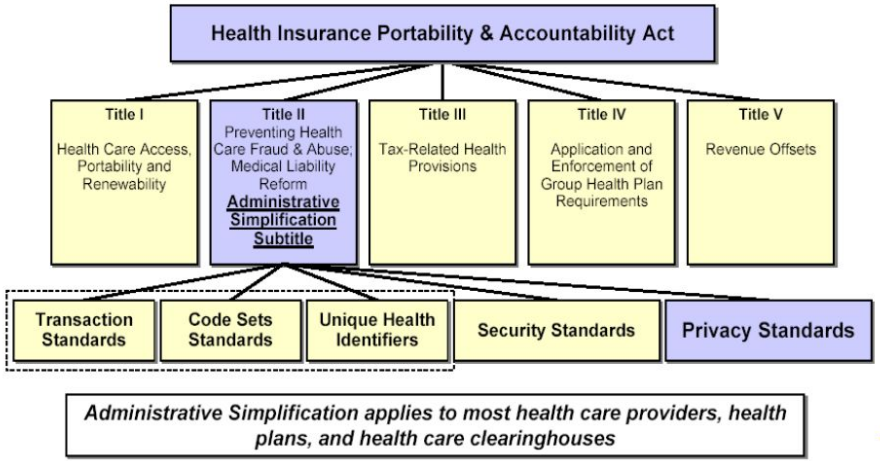
III. Permitted Uses and Disclosures

IV. Patients' Rights to Control their Health Information

V. Administrative Requirements

HIPAA and Privacy Rule Overview:

The Health Insurance Portability and Accountability Act (HIPAA) has many parts. Most relevant to students in the health professions are the "Administrative Simplification" provisions including national standards for electronic health care transactions, codes, identifiers, security, and the privacy of personal health information.



Tổng quan lý thuyết

Introduction to HIPAA for Health Care Professionals

Gerald P. Koocher, Ph.D., ABPP

Content

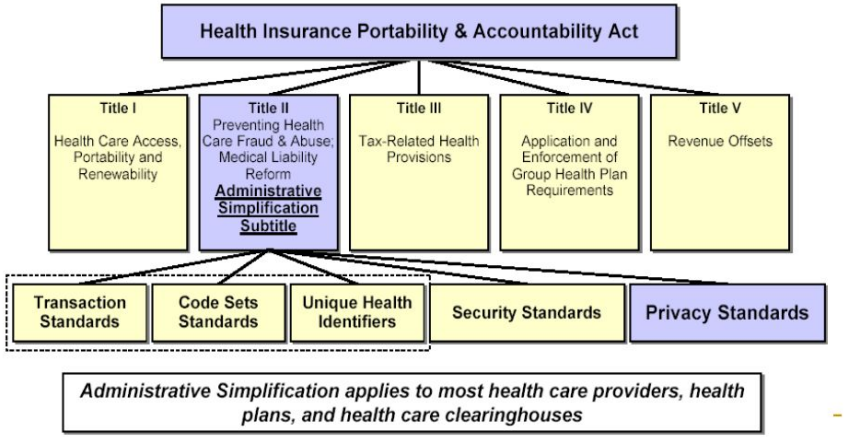
HIPAA

Introduction

- This educational module is intended to help students understand the fundamentals of HIPAA prior to beginning work at clinical sites.

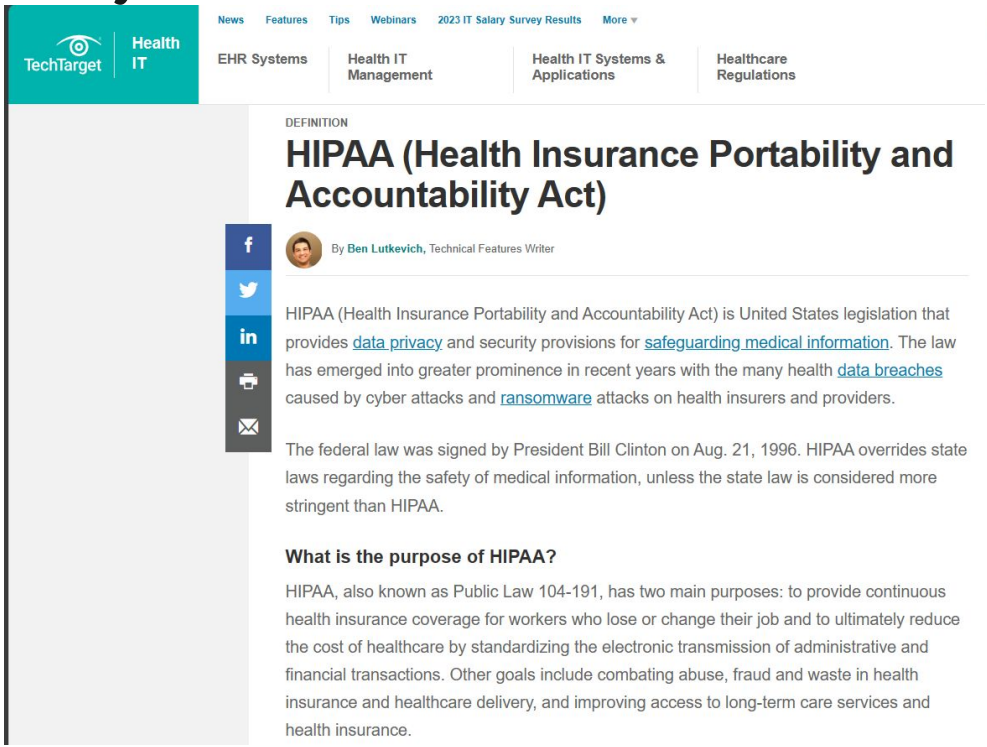
HIPAA and Privacy Rule Overview:

The Health Insurance Portability and Accountability Act (HIPAA) has many parts. Most relevant to students in the health professions are the "Administrative Simplification" provisions including national standards for electronic health care transactions, codes, identifiers, security, and the privacy of personal health information.



Tổng quan lý thuyết

HIPAA



TechTarget | Health IT

News Features Tips Webinars 2023 IT Salary Survey Results More

EHR Systems | Health IT Management | Health IT Systems & Applications | Healthcare Regulations

DEFINITION

HIPAA (Health Insurance Portability and Accountability Act)

By **Ben Lutkevich**, Technical Features Writer

HIPAA (Health Insurance Portability and Accountability Act) is United States legislation that provides data privacy and security provisions for safeguarding medical information. The law has emerged into greater prominence in recent years with the many health data breaches caused by cyber attacks and ransomware attacks on health insurers and providers.

The federal law was signed by President Bill Clinton on Aug. 21, 1996. HIPAA overrides state laws regarding the safety of medical information, unless the state law is considered more stringent than HIPAA.

What is the purpose of HIPAA?

HIPAA, also known as Public Law 104-191, has two main purposes: to provide continuous health insurance coverage for workers who lose or change their job and to ultimately reduce the cost of healthcare by standardizing the electronic transmission of administrative and financial transactions. Other goals include combating abuse, fraud and waste in health insurance and healthcare delivery, and improving access to long-term care services and health insurance.

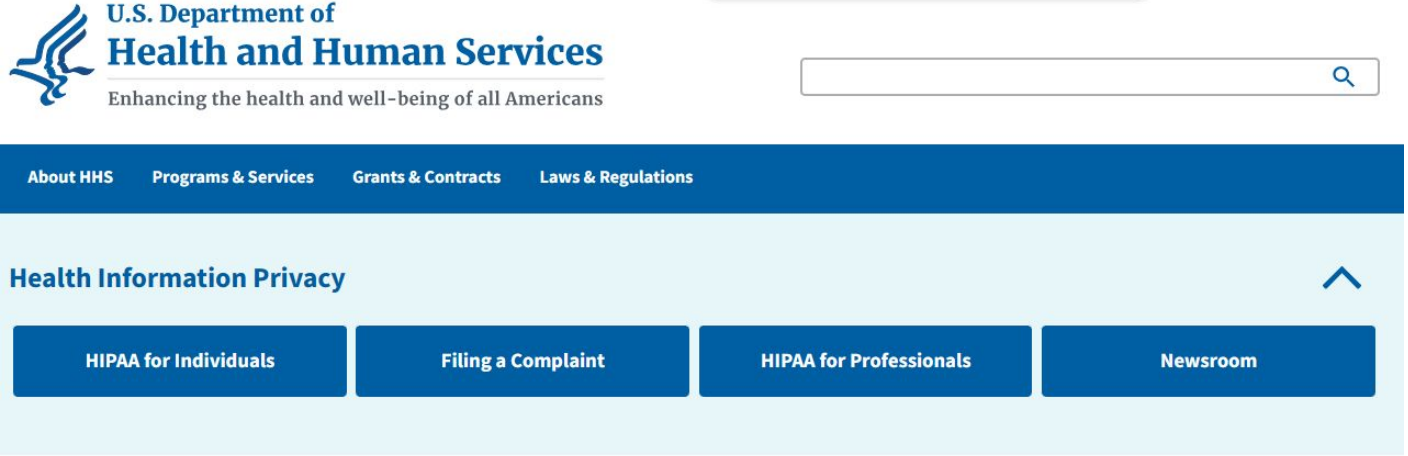
What are the 5 main components of HIPAA?

HIPAA contains five sections, or titles:

- **Title I: HIPAA Health Insurance Reform.** Title I protects health insurance coverage for individuals who lose or change jobs. It also prohibits group health plans from denying coverage to individuals with specific diseases and preexisting conditions and from setting lifetime coverage limits.
- **Title II: HIPAA Administrative Simplification.** Title II directs the U.S. Department of Health and Human Services (HHS) to establish national standards for processing electronic healthcare transactions. It also requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS.
- **Title III: HIPAA Tax-Related Health Provisions.** Title III includes tax-related provisions and guidelines for medical care.
- **Title IV: Application and Enforcement of Group Health Plan Requirements.** Title IV further defines health insurance reform, including provisions for individuals with preexisting conditions and those seeking continued coverage.
- **Title V: Revenue Offsets.** Title V includes provisions on company-owned life insurance and the treatment of those who lose their U.S. citizenship for income tax purposes.

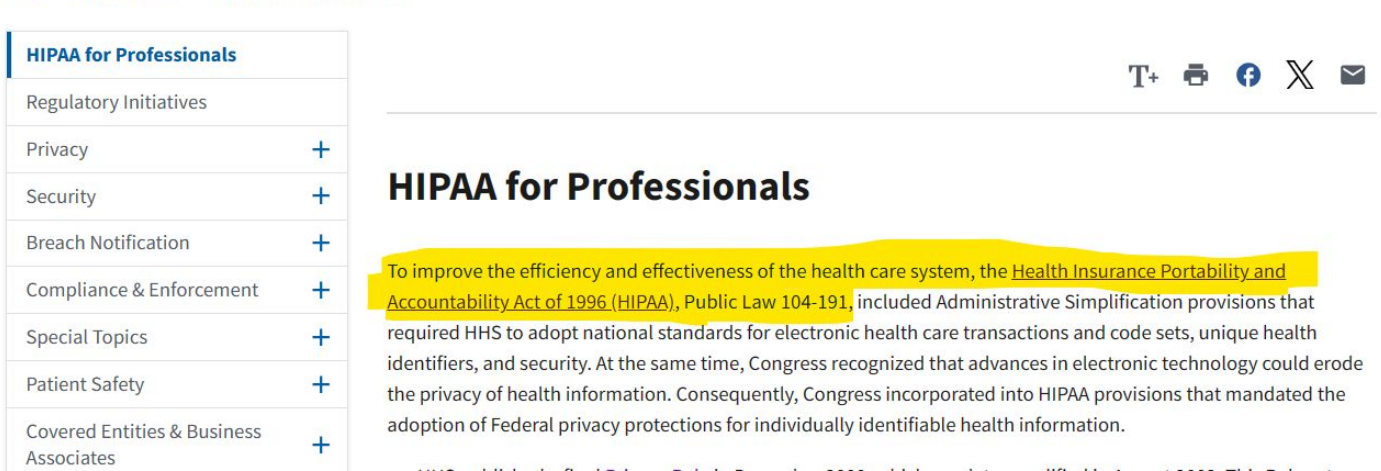
Tổng quan lý thuyết

HIPAA



HIPAA for Professionals | HHS.gov

PLAW-104publ191.pdf (govinfo.gov)



Tổng quan lý thuyết

HIPAA

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.
- View the Combined Regulation Text - PDF (as of March 2013). This is an unofficial version that presents all the HIPAA regulatory standards in one document. The official version of all federal regulations is published in the Code of Federal Regulations (CFR). View the official versions at 45 C.F.R. Part 160 - PDF, Part 162 - PDF, and Part 164 - PDF.

HHS đã công bố **Quy tắc quyền riêng tư** cuối cùng vào tháng 12 năm 2000, sau đó được sửa đổi vào tháng 8 năm 2002. Quy tắc này đặt ra các tiêu chuẩn quốc gia để bảo vệ thông tin sức khỏe có thể nhận dạng cá nhân của ba loại tổ chức được bảo hiểm: chương trình bảo hiểm sức khỏe, cơ quan thanh toán chăm sóc sức khỏe và nhà cung cấp dịch vụ chăm sóc sức khỏe. thực hiện các giao dịch chăm sóc sức khỏe tiêu chuẩn bằng điện tử. Việc tuân thủ Quy tắc về quyền riêng tư được yêu cầu kể từ ngày 14 tháng 4 năm 2003.

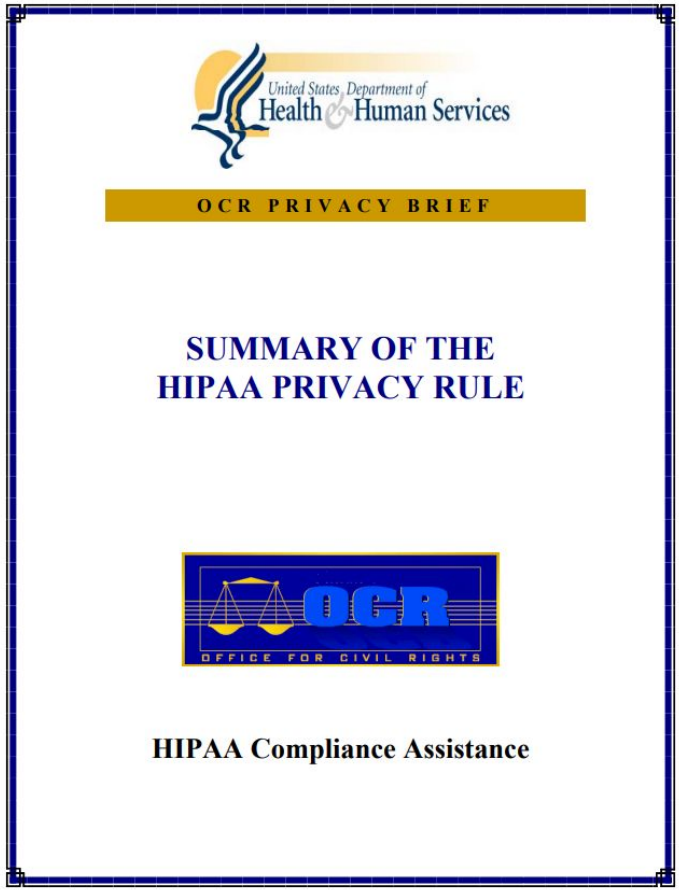
HHS đã công bố **Quy tắc bảo mật** cuối cùng vào tháng 2 năm 2003. Quy tắc này đặt ra các tiêu chuẩn quốc gia để bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin sức khỏe được bảo vệ bằng điện tử. Việc tuân thủ Quy tắc An ninh được yêu cầu kể từ ngày 20 tháng 4 năm 2005.

Quy tắc thực thi cung cấp các tiêu chuẩn cho việc thực thi tất cả các Quy tắc đơn giản hóa hành chính.
HHS đã ban hành quy tắc Omnibus cuối cùng nhằm thực hiện một số điều khoản của Đạo luật HITECH nhằm tăng cường các biện pháp **bảo vệ quyền riêng tư và bảo mật** cho thông tin sức khỏe được thiết lập theo HIPAA, hoàn thiện Quy tắc Thông báo Vi phạm.

Xem Văn bản Quy định Kết hợp - PDF (tính đến tháng 3 năm 2013). Đây là phiên bản không chính thức trình bày tất cả các tiêu chuẩn quy định của HIPAA trong một tài liệu. Phiên bản chính thức của tất cả các quy định liên bang được xuất bản trong Bộ luật Quy định Liên bang (CFR).

Tổng quan lý thuyết

HIPAA


United States Department of Health & Human Services

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

OCR OFFICE FOR CIVIL RIGHTS

HIPAA Compliance Assistance

SUMMARY OF THE HIPAA PRIVACY RULE

Contents

Giới thiệu
Cơ sở pháp lý và quy định
Ai được bảo vệ bởi Quy tắc quyền riêng tư Cộng tác viên kinh doanh
Thông tin nào được bảo vệ
Nguyên tắc chung về sử dụng và tiết lộ
Việc sử dụng và tiết lộ được phép
Việc sử dụng và tiết lộ được phép
Giới hạn việc sử dụng và tiết lộ ở mức tối thiểu cần thiết
Thông báo và các quyền cá nhân khác
Yêu cầu quản trị
Các lựa chọn tổ chức
Các quy định khác: Người đại diện cá nhân và trẻ vị thành niên
Luật Nhà nước
Việc thực thi và hình phạt đối với việc không tuân thủ
Ngày tuân thủ
Bản sao của Quy tắc & Tài liệu
Ghi chú cuối cùng

Tổng quan lý thuyết

HIPAA

Summary of the HIPAA Security Rule

Introduction

Statutory and Regulatory Background

Who is Covered by the Security Rule

Business Associates

What Information is Protected

General Rules

Risk Analysis and Management

Administrative Safeguards

Physical Safeguards

Technical Safeguards

Required and Addressable Implementation Specifications

Organizational Requirements

Policies and Procedures and Documentation Requirements

State Law

Enforcement and Penalties for Noncompliance

Compliance Dates

Copies of the Rule and Related Materials

End Notes

Tóm tắt Quy tắc bảo mật HIPAA

Giới thiệu

Nền tảng pháp lý và quy định

Ai được bảo vệ bởi quy tắc bảo mật

Cộng tác viên kinh doanh

Thông tin nào được bảo vệ

Quy định chung

Phân tích và quản lý rủi ro

Các biện pháp bảo vệ hành chính

Các biện pháp bảo vệ vật lý

Biện pháp bảo vệ kỹ thuật

Thông số kỹ thuật triển khai bắt buộc và có địa chỉ

Yêu cầu tổ chức

Chính sách, thủ tục và yêu cầu về tài liệu

Luật Tiểu bang

Thực thi và hình phạt đối với việc không tuân thủ

Ngày tuân thủ

Bản sao của Quy tắc và Tài liệu liên quan

Ghi chú cuối

Security —

Summary of the Security Rule

Security Guidance

Cyber Security Guidance

Tổng quan lý thuyết

HIPAA

Security
- Summary of the Security Rule
- Security Guidance
- Cyber Security Guidance

Summary of the HIPAA Security Rule

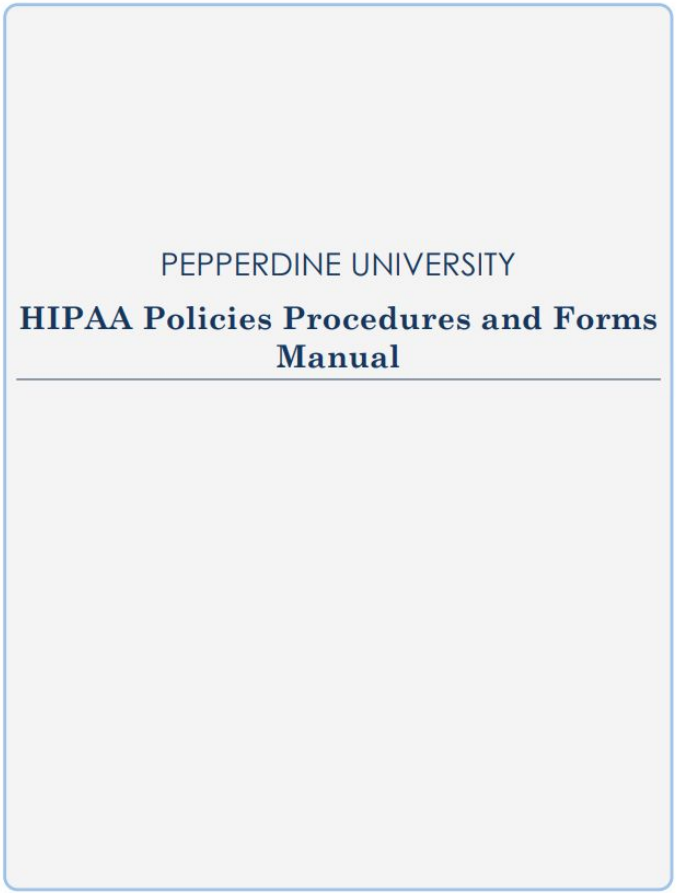
Introduction
Statutory and Regulatory Background
Who is Covered by the Security Rule
Business Associates
What Information is Protected
General Rules
Risk Analysis and Management
Administrative Safeguards
Physical Safeguards
Technical Safeguards
Required and Addressable Implementation Specifications
Organizational Requirements
Policies and Procedures and Documentation Requirements
State Law
Enforcement and Penalties for Noncompliance
Compliance Dates
Copies of the Rule and Related Materials
End Notes

Tóm tắt Quy tắc bảo mật HIPAA

Giới thiệu
Nền tảng pháp lý và quy định
Ai được bảo vệ bởi quy tắc bảo mật
Cộng tác viên kinh doanh
Thông tin nào được bảo vệ
Quy định chung
Phân tích và quản lý rủi ro
Các biện pháp bảo vệ hành chính
Các biện pháp bảo vệ vật lý
Biện pháp bảo vệ kỹ thuật
Thông số kỹ thuật triển khai bắt buộc và có địa chỉ
Yêu cầu tổ chức
Chính sách, thủ tục và yêu cầu về tài liệu
Luật Tiểu bang
Thực thi và hình phạt đối với việc không tuân thủ
Ngày tuân thủ
Bản sao của Quy tắc và Tài liệu liên quan
Ghi chú cuối

Tổng quan lý thuyết

HIPAA



PEPPERDINE UNIVERSITY - HIPAA Policies Procedures and Forms Manual

Table of Contents

PEPPERDINE UNIVERSITY - HIPAA Policies Procedures and Forms Manual

Chính sách
Đại học Pepperdine sẽ thực hiện các biện pháp bảo vệ hành chính, kỹ thuật và vật lý phù hợp để bảo vệ tính bảo mật của thông tin sức khỏe được bảo vệ một cách hợp lý. Các thành phần được chỉ định có liên quan có thể phát triển các chính sách và thủ tục bổ sung nghiêm ngặt hơn các thông số được nêu bên dưới để tối đa hóa quyền riêng tư của thông tin sức khỏe được bảo vệ trong các trường hợp riêng của một thành phần cụ thể.

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.

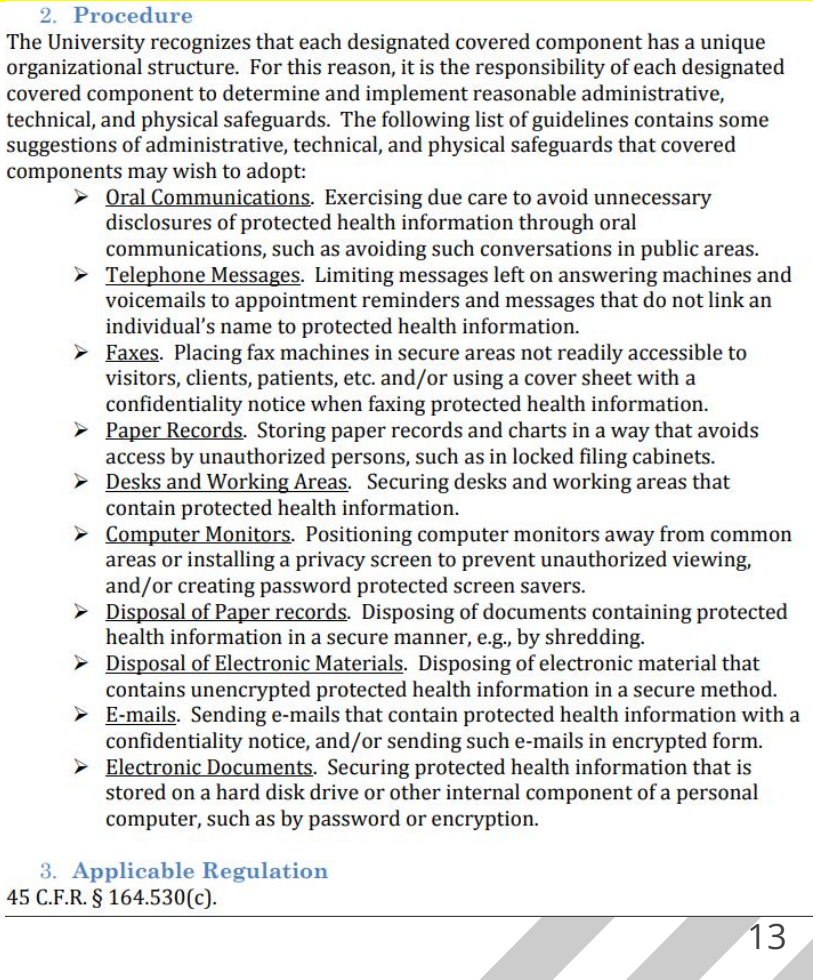
2. Procedure

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.

PEPPERDINE UNIVERSITY - HIPAA Policies Procedures and Forms Manual

Quy trình:
Ø Giao tiếp ngôn ngữ: Thực hiện cẩn thận để tránh những điều không cần thiết tiết lộ thông tin sức khoẻ được bảo vệ bằng ngôn ngữ, chẳng hạn như tránh những cuộc trò chuyện như vậy ở khu vực công cộng.
Ø Tin nhắn điện thoại. Hạn chế tin nhắn để lại trên máy trả lời tự động và thư thoại đến lời nhắc cuộc hẹn và tin nhắn không liên kết tên của cá nhân đối với thông tin sức khỏe được bảo vệ.
Ø Fax. Đặt máy fax ở những khu vực an toàn mà người dân không thể tiếp cận được
những người đến thăm, khách hàng, bệnh nhân, v.v. và/hoặc sử dụng trang bìa có thông báo bảo mật khi gửi fax thông tin sức khỏe được bảo vệ.
Ø Hồ sơ giấy. Lưu trữ hồ sơ giấy và biểu đồ theo cách tránh truy cập trái phép bởi những người không có thẩm quyền, chẳng hạn như trong tủ hồ sơ có khóa.
Ø Bàn làm việc và khu vực làm việc. Bảo vệ bàn làm việc và khu vực làm việc chứa thông tin sức khỏe được bảo vệ.
Ø Màn hình máy tính. Đặt màn hình máy tính cách xa nơi thường dùng khu vực hoặc cài đặt màn hình riêng tư để ngăn chặn việc xem trái phép, và/hoặc tạo trình bảo vệ màn hình được bảo vệ bằng mật khẩu.
Ø Tiêu hủy hồ sơ giấy. Vứt bỏ các tài liệu có chứa dữ liệu được bảo vệ thông tin sức khỏe một cách an toàn, ví dụ như bằng cách băm nhỏ.
Ø Vứt bỏ vật liệu điện tử. Vứt bỏ tài liệu điện tử có chứa thông tin sức khỏe được bảo vệ không được mã hóa theo một phương pháp an toàn.
Ø Thư điện tử. Gửi e-mail có chứa thông tin sức khỏe được bảo vệ bằng thông báo bảo mật và/hoặc gửi những email đó ở dạng được mã hóa.
Ø Chứng từ điện tử. Bảo mật thông tin sức khỏe được bảo vệ được lưu trữ trên ổ đĩa cứng hoặc thành phần bên trong khác của thiết bị cá nhân máy tính, chẳng hạn như bằng mật khẩu hoặc mã hóa



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).

PEPPERDINE UNIVERSITY - HIPAA Policies Procedures and Forms Manual

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

J. Acknowledgement of Receipt of Notice of Privacy Practices

A. Ghi nhận về việc Tiết lộ Thông tin Sức khỏe được bảo vệ

B. Quyền sử dụng/tiết lộ thông tin sức khỏe được bảo vệ

C. Hợp đồng thỏa thuận liên quan

D. Từ chối yêu cầu sửa đổi

E. Từ chối yêu cầu truy cập

F. Khiếu nại về quyền riêng tư

G. Yêu cầu truy cập thông tin sức khỏe được bảo vệ

H. Yêu cầu giải trình các thông tin tiết lộ

I. Yêu cầu sửa đổi thông tin sức khỏe được bảo vệ

J. Xác nhận đã nhận được thông báo về thực hành quyền riêng tư

A. Accounting for Disclosures of Protected Health Information

Date of Disclosure	Name and Address of Person who Received PHI	Reason for Disclosure	Description of PHI Disclosed	Persons or Offices Processing the Accounting

B. 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 re-disclosed 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

_____
Individual's Name (Print)

_____ _____
Name of Legal Representative, if applicable (Print) Relationship

*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 C.F.R. § 164.508(b)(4)(ii)(A&B)).

C. Business Associate Agreement

Pepperdine University
Business Associate Agreement

Definitions:
The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary of Department of Health and Human Services, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:
(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____ **[Insert name of Business Associate].**

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Pepperdine University.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate:
Business Associate agrees to:
(a) Not use or disclose protected health information ("PHI") other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 64 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement;

(c) Report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410, and any security incident of which it becomes aware within seven (7) business days;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Make available PHI in a designated record set to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;

(f) Make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;

(h) To the extent the Business Associate is to carryout one or more of Covered Entity's obligation(s) under Subpart E or 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary of Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate:
(a) Business Associate may only use or disclose PHI as necessary to perform the services set forth in Service Agreement.

(b) Business Associate may use or disclose PHI as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures.

(d) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E or 45 CFR Part 164 if done by Covered Entity.

Provisions for Covered Entity to Inform Business Associate of Notice of Privacy Practices and Restrictions ("NPP"):
(a) Covered Entity shall notify Business Associate of any limitation(s) in the NPP of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

Term and Termination:
(a) Term. The Term of this Agreement shall be effective as of _____ **[Insert effective date]**, and shall terminate on _____ **[Insert termination date]** or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement.

Miscellaneous:
(a) Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law, in equity, or under this Agreement, in the event of any violation by Business Associate of any of the provisions of this Agreement, or any explicit threat thereof, Covered Entity shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

(b) Indemnification. Business Associate shall indemnify, hold harmless, and defend Covered Entity from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of Business Associate in connection with the representations, duties and obligations of Business Associate under this Agreement.

(c) Obligations of Business Associate upon termination. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity, or if agreed to by Covered Entity destroy, all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

(e) The parties agree that the Business Associate Agreement may need to be amended as necessary to accommodate changes to HIPAA or other privacy laws and regulations in the future.

(f) The parties further agree that the Business Associate (and its subcontractors if applicable) is acting as an independent contractor and not as an agent of the Covered Entity.

D. 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*):

_____
_____
_____
_____

_____ _____ _____
Responsible Party's Name (*Print*) Date
Title of the persons or offices responsible for receiving and processing the request

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 the Privacy Official is:

Kim Miller
Pepperdine University
24255 Pacific Coast Highway
Telephone: (310) 506-4208
E-mail: kim.miller@pepperdine.edu

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

E. 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:

_____
_____
_____
_____

_____ _____ _____
Responsible Party's Name (*Print*) Date
Title of the persons or offices responsible for receiving

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 Kim Miller at 24255 Pacific Coast Highway, Malibu, California 90263, (310) 506-4208 or kim.miller@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

_____
Name of Individual or Legal Representative (*Print*)

F. 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:

Kim Miller
HIPAA Privacy Official
24255 Pacific Coast Highway
Malibu, CA 90263

You may also submit the complaint electronically to kim.miller@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.

G. 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 Numbers:_____

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

_____
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.

H. Request for Accounting of Disclosures

I understand that I have the right to an accounting of uses and disclosures of my Protected Health Information for purposes other than treatment, payment, and health care operations. I understand that the University's responsibility for such an accounting became effective April 14, 2003, and that accounting for disclosures prior to that date is not available. I understand that a fee may be charged for more than one accounting in a 12-month period.

Name:_____ Date:_____

I hereby request an accounting of disclosures of my Protected Health Information from _____ to _____ (*if known, name and address of entity*) maintained by Pepperdine University, _____ (*name of department*).

Please provide a brief description of the Protected Health Information disclosed:

Please provide a brief statement of the purpose of the disclosure; or in lieu of such statement, a copy of a written request for disclosure, if any.

_____
Signature of Individual (*or Legal Representative*) Date

_____
Individual's Name (*Print*)

_____
Name of Legal Representative, *if applicable* (*Print*) Relationship to Individual

_____
Responsibility Party's Name (*Print*)
Title of the persons or offices responsible for receiving and processing the request

_____
Date

I. Request for Amendment to Protected Health Information

Name:_____ Date:_____

Telephone Numbers:_____

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

_____
Individual's Name (*Print*)

_____
Name of Legal Representative, *if applicable* (*Print*) Relationship to Individual

_____
Responsibility Party's Name (*Print*)
Title of the persons or offices responsible for receiving and processing the request

_____
Date

J. Acknowledgement of Receipt of Notice of Privacy Practices

Name:_____

Address:_____

Facility Name:_____

I acknowledge that I have received or been offered a copy of Pepperdine University's NPP which describes how my PHI is used and shared. I understand that Pepperdine University has the right to change this NPP at any time. I may obtain a current copy by contacting the Department in which my care was provided or by visiting Pepperdine University's website at http://www.pepperdine.edu/provost/content/policies/hipaa_manual_5_2012.pdf.

My signature below acknowledges that I have been offered a copy or provided with a copy of the NPP:

_____

Signature of Patient Date

_____

Print Name

_____

Personal Representative's Title *(e.g., Guardian, Executor of Estate, Health Care Power of Attorney)*

For Department Use Only: Complete this section if you are unable to obtain a signature.

- If the patient or personal representative is unable or unwilling to sign this *Acknowledgement*, or the *Acknowledgement* is not signed for any other reason, state the reason:

  _____

  _____

- Describe the steps taken to obtain the patient's (or personal representative's) signature on the *Acknowledgement:*

  _____

  _____

Case study 2: VINMEC - Policies for the protection of Protected Health Information (PHI)

A crucial aspect of HIPAA compliance is understanding what constitutes Protected Health Information. According to the U.S.

HIPAA regulations outline 18 specific identifiers that must be removed from health information to render it de-identified. Some common examples include:

Name and address,
Social Security number (SSN),
Date of birth (DOB), Email addresses,
phone numbers, and fax numbers,
Medical record numbers or account numbers,
Fingerprints or facial images,
Certificate/license numbers, etc.

Ensuring the protection of PHI is crucial for myriad reasons, most fundamentally:

- patient privacy
- data security
- Federal Compliance

Maintaining the privacy and security of Protected Health Information is essential to upholding HIPAA regulations.

- Vinmec is a private healthcare system in Vietnam, invested by Vingroup Corporation – Vietnam's leading private economic consortium.

- Vinmec has a network of 10 hospitals and clinics across the country, offering a wide range of medical services, including preventive care, diagnosis, treatment, and rehabilitation.

- Vinmec is committed to providing high-quality healthcare services to all Vietnamese people.

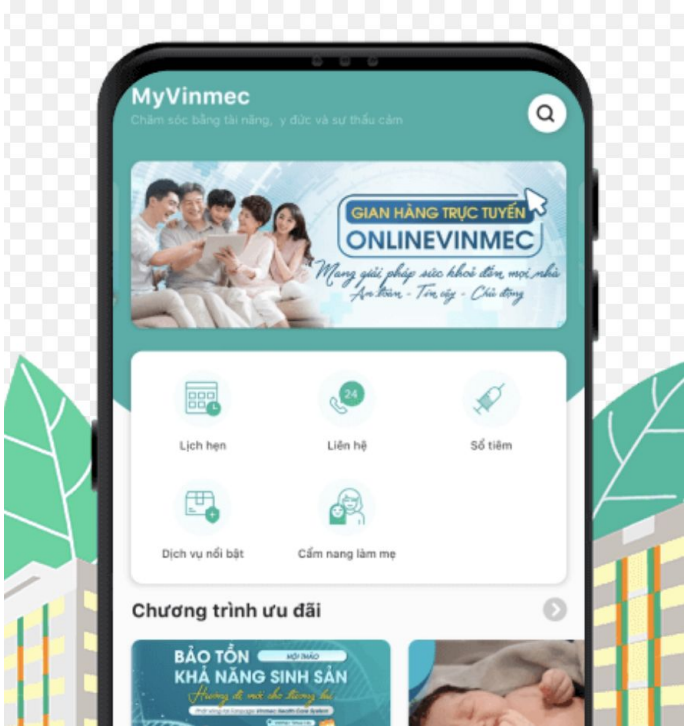
VINMEC
HEALTHCARE SYSTEM

Vinmec provides a privacy policy describes how Vinmec International General Hospital Joint Stock Company collects, receives, summarizes, stores, uses, processes, discloses, shares, and ensures the security of Customer Information of organizations and individuals, including customers, agents, suppliers, contractors, and partners:

- (i) using the services provided directly at Vinmec medical examination and treatment facilities or other services provided by Vinmec and Vingroup;

- (ii) accessing and using customer interaction channels owned by Vinmec, including but not limited to: website www.vinmec.com, My Vinmec application, websites and groups on social media (such as Facebook, ...) owned by Vinmec ("Vinmec Channels").

The General Principles section also provides some specific details about how Vinmec collects and uses Customer Information.



Vinmec uses Customer Information for a variety of purposes, including:

- Providing and improving Vinmec services.
- Communicating with customers.
- Providing customer support.
- Conducting research and development.

Vinmec shares Customer Information with third parties in a limited number of cases, such as:

- When necessary to provide a service or product requested by the customer.
- When required by law.
- When Vinmec has the customer's consent.

Vinmec takes steps to protect the security of Customer Information, including:

- Using physical, technical, and administrative security measures to protect Customer Information.
- Limiting access to Customer Information to authorized personnel.

Customers have the right to access and correct their Customer Information.
Customers can also opt out of receiving marketing communications from Vinmec.

The process of storing cells in Vinmec Cord Blood Bank

Figure 1: The process of storing human's cells in Vinmec in closed process

Vinmec Cord Blood Bank is the first and only cord blood bank in Vietnam to be accredited by the American Association of Blood Banks (AABB). The bank uses state-of-the-art technology to ensure the safety and quality of its stored cord blood.

Vinmec Cord Blood Bank offers a variety of services, including:

- Cord blood collection and storage
- Cord blood banking for personal use
- Cord blood banking for public use
- Cord blood research

The bank is committed to providing families with access to the best possible cord blood banking services

The process of storing cells is finalize in steps:

1. The customer learns about stem cell storage services.
2. Collect customer information.
3. Sign contract.
4. Collect, deliver and process object.
5. Store samples and manage customer information.

4. Ngân hàng lưu trữ tế bào gốc Vinmec: chi phí

Chi phí lưu trữ tế bào gốc của Vinmec được thể hiện chi tiết qua bảng sau:

THÔNG TIN VỀ CÁC GÓI

DỊCH VỤ	PHÍ (VNĐ)	
	01 mẫu	02 mẫu
Gói Máu cuống rốn (bao gồm thu thập, xử lý, lưu trữ)		
GÓI-MCR - 1 năm	30,000,000	57,000,000
GÓI-MCR - 5 năm liên tục	40,000,000	77,000,000
GÓI-MCR - 10 năm liên tục	54,000,000	105,000,000
GÓI-MCR - 15 năm liên tục	70,000,000	137,000,000
GÓI-MCR - 20 năm liên tục	85,000,000	167,000,000
GÓI-MCR - 25 năm liên tục	90,000,000	177,000,000
Gói Dây rốn (bao gồm thu thập, xử lý, lưu trữ)		
GÓI-DR - 1 năm	65,000,000	120,000,000
GÓI-DR - 5 năm liên tục	79,000,000	148,000,000
GÓI-DR - 10 năm liên tục	100,000,000	190,000,000
GÓI-DR - 15 năm liên tục	116,000,000	223,000,000
GÓI-DR - 20 năm liên tục	120,000,000	230,000,000
GÓI-DR - 25 năm liên tục	122,000,000	235,000,000

- The activities of the Umbilical Cord Blood Bank are operated in a closed, professional, and modern process.

- The closed process involves close coordination between the umbilical cord blood bank and the operating room/delivery room. This coordination helps to ensure that the collection of umbilical cord blood is carried out in a timely and safe manner.

- Besides, Vinmec ensures Maximum security with a high-tech security system, which states that the umbilical cord blood bank uses a high-tech security system to protect the privacy of its customers and their umbilical cord blood samples.

PRUDENTIAL - HIPAA Notice of Privacy Practices

General Policy

PRUDENTIAL are required by law to:

- Ensure that Protected Health Information that identifies you is kept private, except as such information is required or permitted to be disclosed by law.
- Describe the Plans' legal duties and privacy practices with respect to your Protected Health Information. Abide by the terms of this Notice that are currently in effect.
- Inform you in the event of a breach of your unsecured Protected Health Information

PRUDENTIAL - HIPAA Notice of Privacy Practices

Scope

PRUDENTIAL must follow the terms of the Notice currently in effect. Our employees, agents and authorized vendors who have access to your Protected Health Information to provide services must also follow this Notice.

PRUDENTIAL - HIPAA Notice of Privacy Practices

Safeguarding Protected Health Information

For Treatment : PRUDENTIAL do not provide treatment to customer, but PRUDENTIAL may still use and disclose Protected Health Information for treatment purposes.
For Payment : PRUDENTIAL may also use and disclose customer's health information for payment purposes, such as to make sure that claims are paid accurately, and customer receive the correct benefits
For Health Care Operations : PRUDENTIAL may also use and disclose Protected Health Information for our health care operations to ensure quality and efficient plan operations, which include plan administration, quality assessment and improvement, vendor review and for health care fraud and abuse detection and compliance

PRUDENTIAL - HIPAA Notice of Privacy Practices

Safeguarding Protected Health Information

Uses and Disclosures of Protected Health Information Without Individual Authorization

- When PRUDENTIAL disclose customer's information to customer.
- To PRUDENTIAL's business associates who perform services for us that require access to customer's health information.
- Where disclosure is required by law.
- To a public health authority authorized by law to collect or receive your information to prevent or control disease, injury or disability or when reviewing reports of child abuse or for the conduct of other authorized public health activities and responsibilities.
- To a health oversight agency for such activities.
- For judicial and administrative proceedings.

PRUDENTIAL - HIPAA Notice of Privacy Practices

Individual Rights With Respect To Your Protected Health Information

- RIGHT TO REQUEST RESTRICTIONS
- RIGHT TO ALTERNATIVE CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION
- RIGHT TO INSPECT AND COPY PROTECTED HEALTH INFORMATION
- RIGHT TO AMEND PROTECTED HEALTH INFORMATION
- RIGHT TO AN ACCOUNTING
- RIGHT TO A PAPER COPY OF THIS NOTICE

PRUDENTIAL - HIPAA Notice of Privacy Practices

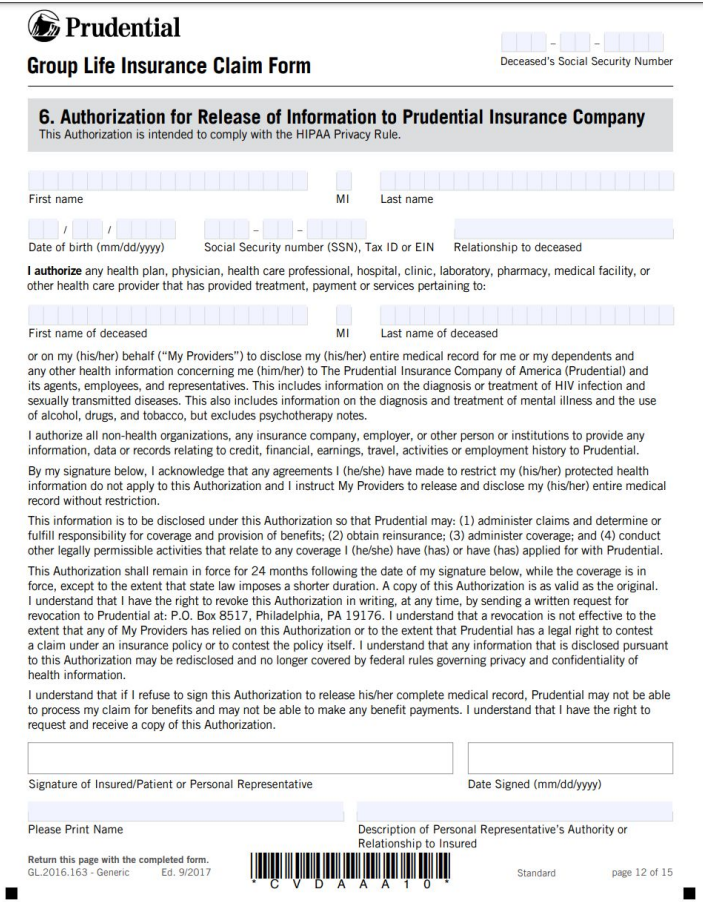
Safeguarding Protected Health Information

Uses and Disclosures of Protected Health Information Without Individual Authorization

- To a medical examiner for the purpose of identifying a deceased person, determining the cause of death, or other duties authorized by law.
- To organ donor organizations in order to aid in such donations.
- For certain research purposes authorized by and subject to federal law.
- To avert a serious threat to health or safety.
- To government officials regarding military personnel and certain domestic and foreign government officials for certain functions authorized by federal law.
- To comply with workers' compensation and other similar programs.

PRUDENTIAL - HIPAA Notice of Privacy Practices

Sample Form



Prudential

Group Life Insurance Claim Form

Deceased's Social Security Number

6. Authorization for Release of Information to Prudential Insurance Company
This Authorization is intended to comply with the HIPAA Privacy Rule.

First name | MI | Last name

Date of birth (mm/dd/yyyy) | Social Security number (SSN), Tax ID or EIN | Relationship to deceased

I authorize any health plan, physician, health care professional, hospital, clinic, laboratory, pharmacy, medical facility, or other health care provider that has provided treatment, payment or services pertaining to:

First name of deceased | MI | Last name of deceased

or on my (his/her) behalf ("My Providers") to disclose my (his/her) entire medical record for me or my dependents and any other health information concerning me (him/her) to The Prudential Insurance Company of America (Prudential) and its agents, employees, and representatives. This includes information on the diagnosis or treatment of HIV infection and sexually transmitted diseases. This also includes information on the diagnosis and treatment of mental illness and the use of alcohol, drugs, and tobacco, but excludes psychotherapy notes.

I authorize all non-health organizations, any insurance company, employer, or other person or institutions to provide any information, data or records relating to credit, financial, earnings, travel, activities or employment history to Prudential.

By my signature below, I acknowledge that any agreements I (he/she) have made to restrict my (his/her) protected health information do not apply to this Authorization and I instruct My Providers to release and disclose my (his/her) entire medical record without restriction.

This information is to be disclosed under this Authorization so that Prudential may: (1) administer claims and determine or fulfill responsibility for coverage and provision of benefits; (2) obtain reinsurance; (3) administer coverage; and (4) conduct other legally permissible activities that relate to any coverage I (he/she) have (has) or have (has) applied for with Prudential.

This Authorization shall remain in force for 24 months following the date of my signature below, while the coverage is in force, except to the extent that state law imposes a shorter duration. A copy of this Authorization is as valid as the original. I understand that I have the right to revoke this Authorization in writing, at any time, by sending a written request for revocation to Prudential at: P.O. Box 8517, Philadelphia, PA 19176. I understand that a revocation is not effective to the extent that any of My Providers has relied on this Authorization or to the extent that Prudential has a legal right to contest a claim under an insurance policy or to contest the policy itself. I understand that any information that is disclosed pursuant to this Authorization may be redisclosed and no longer covered by federal rules governing privacy and confidentiality of health information.

I understand that if I refuse to sign this Authorization to release his/her complete medical record, Prudential may not be able to process my claim for benefits and may not be able to make any benefit payments. I understand that I have the right to request and receive a copy of this Authorization.

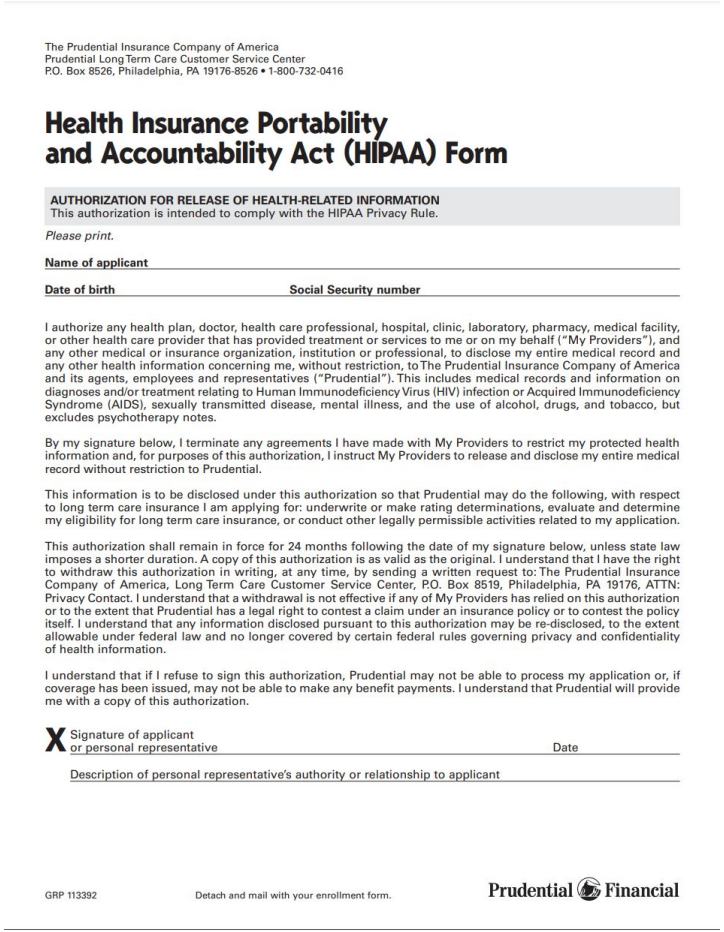
Signature of Insured/Patient or Personal Representative | Date Signed (mm/dd/yyyy)

Please Print Name | Description of Personal Representative's Authority or Relationship to Insured

Return this page with the completed form.
GL.2016.163 - Generic Ed. 9/2017 *CVDAAA10* Standard page 12 of 15

PRUDENTIAL - HIPAA Notice of Privacy Practices

Sample Form



The Prudential Insurance Company of America
Prudential Long Term Care Customer Service Center
P.O. Box 8526, Philadelphia, PA 19176-8526 • 1-800-732-0416

Health Insurance Portability and Accountability Act (HIPAA) Form

AUTHORIZATION FOR RELEASE OF HEALTH-RELATED INFORMATION
This authorization is intended to comply with the HIPAA Privacy Rule.

Please print.

Name of applicant _____

Date of birth _____ **Social Security number** _____

I authorize any health plan, doctor, health care professional, hospital, clinic, laboratory, pharmacy, medical facility, or other health care provider that has provided treatment or services to me or on my behalf ("My Providers"), and any other medical or insurance organization, institution or professional, to disclose my entire medical record and any other health information concerning me, without restriction, to The Prudential Insurance Company of America and its agents, employees and representatives ("Prudential"). This includes medical records and information on diagnoses and/or treatment relating to Human Immunodeficiency Virus (HIV) infection or Acquired Immunodeficiency Syndrome (AIDS), sexually transmitted disease, mental illness, and the use of alcohol, drugs, and tobacco, but excludes psychotherapy notes.

By my signature below, I terminate any agreements I have made with My Providers to restrict my protected health information and, for purposes of this authorization, I instruct My Providers to release and disclose my entire medical record without restriction to Prudential.

This information is to be disclosed under this authorization so that Prudential may do the following, with respect to long term care insurance I am applying for: underwrite or make rating determinations, evaluate and determine my eligibility for long term care insurance, or conduct other legally permissible activities related to my application.

This authorization shall remain in force for 24 months following the date of my signature below, unless state law imposes a shorter duration. A copy of this authorization is as valid as the original. I understand that I have the right to withdraw this authorization in writing, at any time, by sending a written request to: The Prudential Insurance Company of America, Long Term Care Customer Service Center, P.O. Box 8519, Philadelphia, PA 19176, ATTN: Privacy Contact. I understand that a withdrawal is not effective if any of My Providers has relied on this authorization or to the extent that Prudential has a legal right to contest a claim under an insurance policy or to contest the policy itself. I understand that any information disclosed pursuant to this authorization may be re-disclosed, to the extent allowable under federal law and no longer covered by certain federal rules governing privacy and confidentiality of health information.

I understand that if I refuse to sign this authorization, Prudential may not be able to process my application or, if coverage has been issued, may not be able to make any benefit payments. I understand that Prudential will provide me with a copy of this authorization.

X Signature of applicant or personal representative _____ Date _____

Description of personal representative's authority or relationship to applicant _____

GRP 113392 Detach and mail with your enrollment form. Prudential Financial

PRUDENTIAL - HIPAA Notice of Privacy Practices

Case Study

Potential HIPAA Right of Access Violation Settled for $80,000

Posted By Steve Alder on Aug 28, 2023

The UnitedHealthcare Insurance Company (UHIC) has agreed to settle an alleged failure to provide timely access to Protected Health Information for $80,000. The voluntary resolution agreement also requires the company to comply with a Corrective Action Plan for a minimum of a year.

In 2019, the Department of Health and Human Services' Office for Civil Rights (OCR) launched an enforcement initiative in response to an increasing number of complaints alleging violations of 45 CFR §164.524 – the access of individuals to Protected Health Information (PHI). To date, the agency has investigated hundreds of complaints and reached settlement agreements in forty-five cases.

The latest settlement agreement relates to a complaint made against UHIC by a customer who had requested a copy of their PHI in January 2021. When the request was not responded to within the allowed time, the customer complained to OCR. The agency initiated an investigation in April 2021, but it was not until July that the customer received the PHI they had requested six months earlier.

PRUDENTIAL - HIPAA Notice of Privacy Practices

Case Study

Aetna Hit with $1 Million HIPAA Fine for Three Data Breaches

Posted By Steve Alder on Oct 29, 2020

Aetna Life Insurance Company and the affiliated covered entity (Aetna) has agreed to settle multiple potential HIPAA violations with the Department of Health and Human Services' Office for Civil Rights (OCR) that were discovered during the investigation of three data breaches that occurred in 2017.

The first of those data breaches was reported to OCR in June 2017 and concerned the exposure of the protected health information (PHI) of health plan members over the Internet. Two web services were used to display health plan-related documents to its members, but those documents could be accessed over the Internet without the need for any login credentials.

The lack of authentication allowed the documents to be indexed by search engines and displayed in search results. Aetna's investigation revealed the PHI of 5,002 individuals had been exposed, which included names, insurance identification numbers, claim payment amounts, procedures service codes, and dates of service.

The second two HIPAA breaches involved the exposure and impermissible disclosure of highly sensitive information in two mailings to plan members. In both mailings, window envelopes had been used which allowed PHI to be viewed without opening the envelopes.

PRUDENTIAL - HIPAA Notice of Privacy Practices

Case Study

$2.2 Million Settlement for Impermissible Disclosure of ePHI

Posted By Steve Alder on Jan 19, 2017

The U.S. Department of Health and Human Services' Office for Civil Rights has agreed a $2.2 million settlement with MAPFRE Life Assurance Company of Puerto Rico – A subsidiary of MAPFRE S.A., of Spain – to resolve potential noncompliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The settlement relates to the impermissible disclosure of the electronic protected health information of 2,209 patients in 2011. On September 29, 2011, a portable USB storage device (pen drive) was left overnight in the IT Department from where it was stolen. The device contained a range of patients' ePHI, including full names, Social Security numbers and dates of birth. The device was not protected by a password and data on the device were not encrypted.

MAPFRE Life reported the device theft to OCR, which launched an investigation to determine whether HIPAA Rules had been violated, as is customary with all breaches of ePHI that impact more than 500 individuals.

Conclusion

HIPAA (Health Insurance Portability and Accountability Act) plays a crucial role in ensuring the protection of individuals' health information by both healthcare providers and companies, including insurance companies like Prudential. The key takeaways regarding HIPAA compliance in safeguarding citizens' health information by these entities are: Privacy and Confidentiality, Authorization and Informed Consent, Data Security, Employee Train-ing and Awareness, Breach Response and Reporting, Patient Rights, Regular Updates and Compliance Reviews.

Overall, HIPAA establishes a comprehensive framework for protecting the privacy and security of individuals' health information, with a focus on informed consent, data security, employee training, and breach response. Compliance with HIPAA is vital in maintaining trust and confidence between individuals, healthcare providers, and insurance companies, ultimately ensuring the safeguarding of citizens' health information

Tài liệu tham khảo:

1. HIPAA Home | HHS.gov : https://www.hhs.gov/hipaa/index.html
2. https://www.hipaajournal.com/
3. https://thuvienphapluat.vn/van-ban/The-thao-Y-te/Luat-kham-benh-chua-benh-nam-2009-98714.aspx
4. https://www.proofpoint.com/us/threat-reference/hipaa-compliance
5. https://online.vinmec.com/chinh-sach-quyen-rieng-tu
6. https://songkhoe.medplus.vn/ngan-hang-luu-tru-te-bao-goc-vinmec-thong-tin-tu-a-z/
7. https://www.vinmec.com/vi/ngan-hang-mo-vinmec/thong-tin-suc-khoe/quy-trinh-luu-tru-mau-cuong-n-tai-vinmec/
8. PLAW-104publ191.pdf (govinfo.gov)
9. HIPPA Policies, Procedures, and Forms Manual (pepperdine.edu)
10. https://www.prudential.com/links/hipaa

Cảm ơn thầy và cả lớp đã theo dõi.