Ho Chi Minh University of Technology
Faculty of Computer Science and Engineering


**LAWS, POLICIES AND STANDARDS IN CYBER - SECURITY**

---

# Assignment

**Health Insurance Portability and Accountability Act (HIPAA)**

---

Instructor:
Dr. Phan Trong Nhan

Authors:
Trn Hoàng Nguyên - 2270012
Đinh Thanh Phong - 2270243
Phm Đăng Khoa - 2171053

# Contents

# 1 Introduction

## 1.1 HIPAA overview

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.

Other HIPAA Administrative Simplification Rules are administered and enforced by the Centers for Medicare and Medicaid Services, and include:
Transactions and Code Sets Standards
Employer Identifier Standard
National Provider Identifier Standard

## 1.2 Assignment objective and scope

This assignment will survey some example for implement in real business and research institute. HIPAA can apply in many field such as:
Research institute.
Hospital.
Insurance provider.
...

# 2 Case studies

## 2.1 PEPPERDINE - HIPAA Policies Procedures and Forms Manual

### 2.1.1 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.

### 2.1.2 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:
• Athletic Training Center;
• Boone Center for the Family;
• Disability Services Office;
• Human Resources, Benefits Department;
• Pepperdine Community Counseling Center;
• Pepperdine Jerry B.H. Union Rescue Clinic;
• Pepperdine Psychology and Education Clinic;
• Student Counseling; and
• Student Health Center.
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.1 However, a designated covered component may not delete sections of these policies and procedures without first consulting the Privacy Official or the Security Official.

### 2.1.3 Safeguarding Protected Health Information

A. 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.

B.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.

### 2.1.4 HIPAA Sample Forms

- 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

### 2.1.5 Sample Forms

### *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.

### *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;

### *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*)

_____ _____

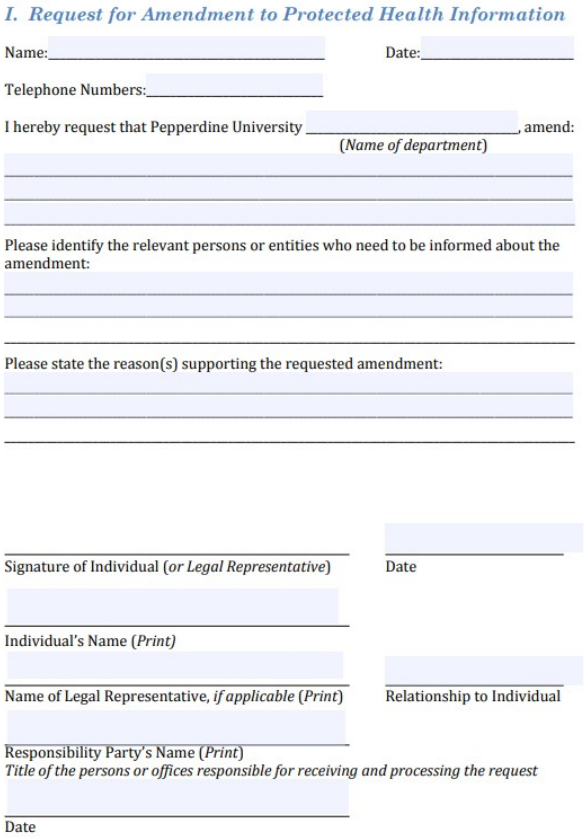
Name of Legal Representative, *if applicable* (*Print*) Relationship to Individual

_____

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:*

## 2.2 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. Department of Health and Human Services, Protected Health Information (PHI) refers to any individually identifiable health information held or transmitted by a covered entity or its business associate. This includes data in electronic, paper, or oral form. PHI encompasses medical records, billing details, treatment plans, laboratory results, insurance claims data—essentially any information related to an individual's physical or mental health condition.

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, and compliance:

- **Patient Privacy**: Ensuring patient confidentiality is critical to maintaining trust between healthcare providers and patients. Unauthorized access to personal health information can lead to embarrassment or stigma for individuals whose private details are exposed.
- **Data Security**: Healthcare organizations store vast amounts of sensitive patient data that can be lucrative targets for cybercriminals seeking financial gain through identity theft or fraud schemes. Safeguarding PHI helps prevent unauthorized access and potential breaches.
- **Federal Compliance**: Failure to comply with HIPAA regulations can result in severe penalties such as fines of up to 1.5 million USD per violation category per year (source), reputational damage, and even criminal charges.

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.

### 2.2.1 General Policy

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's 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").

Customer information is any information or data that can be used to identify the Customer or on the basis of which the Customer is identified, such as name, nationality, phone number, payment card and bank details, personal preferences, email address, location, image, ID information/identity card, date of birth, marital status, insurance information, transaction information, access history, customer journey, biometric data, medical/health records. Customers have read, understood, and agreed to the content of this Privacy Policy. At any time, Vinmec may modify, supplement, and/or update this Privacy Policy. Vinmec will post the modified, supplemented, and/or updated Privacy Policy on the website www.vinmec.com. Continuing to use, access Vinmec Channels, and continue to use the Services is understood to be the Customer's agreement to the content of the modified, supplemented, and/or updated Privacy Policy.

This Privacy Policy includes the following contents:

- Customer Information collected by Vinmec.
- How Vinmec protects Customer Information.
- How Vinmec shares Customer Information.
- Access and choice.
- Contact information, notification, and modification.
- Additional information for Europe.

The General Principles section of Vinmec's Privacy Policy sets forth the following key points:

- Vinmec collects, receives, summarizes, stores, uses, processes, discloses, shares, and ensures the security of Customer Information of organizations and individuals.
- Customer Information is any information or data that can be used to identify the Customer or on the basis of which the Customer is identified.
- Customers must read, understand, and agree to the Privacy Policy before using Vinmec's services.
- Vinmec may modify, supplement, and/or update the Privacy Policy at any time.


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

The General Principles section also provides some specific details about how Vinmec collects and uses Customer Information. For example, Vinmec collects Customer Information when customers:

- Use Vinmec's website or mobile app.
- Sign up for a Vinmec service.
- Provide feedback or contact Vinmec customer service.

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

- Providing and improving Vinmec's 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.

Additional information for customers in Europe is also included, such as:

- Vinmec is committed to complying with the General Data Protection Regulation (GDPR).
- Customers have the right to request access to their Customer Information, to correct their Customer Information, to request the deletion of their Customer Information, and to object to the processing of their Customer Information.

### 2.2.2 An example: The process of storing cells in Vinmec Cord Blood Bank

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 described as below:**

- When customers are interested in learning about the umbilical cord blood stem cell storage service, please contact Vinmec Stem Cell Bank. The staff will arrange a convenient appointment for you. At this appointment, a specialist doctor from Vinmec's umbilical cord blood stem cell bank will provide you with the necessary information such as: What are stem cells and umbilical cord stem cells?, Why is it necessary to store stem cells?, How to store stem cells?, The cost of storing stem cells?, The health conditions of the mother and baby for stem cell collection?, Is it dangerous to collect umbilical cord blood stem cells?...
- After customers choose the umbilical cord blood stem cell storage service at Vinmec MCR Bank. Vinmec MCR Bank will conduct a check and collect customer health information. Doctors at Vinmec Hospital will check the health conditions of customers to see if they are suitable for umbilical cord blood stem cell storage.
- Through the inspection process, customers will sign a storage contract for the period of time they choose. Customers who have been evaluated as having the necessary health conditions for umbilical cord blood stem cell storage will sign a stem cell storage contract with Vinmec MCR Bank.
- The baby's umbilical cord blood will be collected by Vinmec's MCR bank staff/doctors immediately in the delivery room/operating room to ensure the sample is collected in a sterile manner. The collection time is usually from 2 to 3 minutes after the baby is born.
- After collection, the umbilical cord blood will be transported to Vinmec Stem Cell Bank for processing and storage within 48 hours. The entire transportation process is carried out strictly to ensure the quality of the MCR sample. Currently, Vinmec Hospital System is affiliated with many reputable hospitals across the country. Customers can be completely assured when using the umbilical cord blood stem cell storage service even if they do not give birth at Vinmec Hospital System. After collection, the umbilical cord blood will be transported to Vinmec umbilical cord blood bank. After that, it will be processed and stored within 48 hours.

- The umbilical cord blood transported to Vinmec's Stem Cell Bank will be processed and stored. The processing process is carried out in a closed environment in a sterile environment to minimize risks during processing. Quality control tests of the MCR sample are performed during MCR processing.
- All information about the umbilical cord blood stem cell sample stored and customer information are kept strictly confidential. The MCR Bank only provides information on the status of the MCR stem cell sample being stored when requested by the customer or person authorized by the customer in writing.
- When customers need to transplant umbilical cord blood stem cells at Vinmec Hospital, the umbilical cord blood bank will thaw the stem cell sample and process the stem cell sample before proceeding with the transplant. The thawing and processing process is carried out strictly in a completely sterile environment to ensure the quality of the stem cell sample for transplantation.

To conclude, the process is a comprehensive and closed processing and storage process. The activities of the Umbilical Cord Blood Bank are operated in a closed, professional, and modern process. With a closed process, in close coordination between the stem cell bank and the operating room/delivery room, the collection of umbilical cord blood is carried out proactively, in a sterile environment, to minimize risks during collection and storage. With a closed process, in close coordination between the stem cell bank and the operating room/delivery room, the collection of umbilical cord blood is carried out proactively, in a sterile environment, to minimize risks during collection and storage. 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.

## 2.3 PRUDENTIAL - HIPAA Notice of Privacy Practices

### 2.3.1 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.

### 2.3.2 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.

### 2.3.3 Safeguarding Protected Health Information

A. Policy

Treatment, Payment, and Health Care Operations

- **For Treatment**: PRUDENTIAL do not provide treatment to customer, but PRUDENTIAL may still use and disclose Protected Health Information for treatment purposes. For example,

PRUDENTIAL may disclose customer's health information to health care providers, such as doctors, hospitals and other caregivers who request it in connection with providing customer's treatment.

- **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 example, PRUDENTIAL may use and disclose customer's Protected Health Information to determine plan eligibility and responsibility for coverage and benefits. PRUDENTIAL may also use customer's Protected Health Information for utilization review activities.
- **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. For example, PRUDENTIAL may use and disclose your Protected Health Information to assist in the evaluation of a vendor who processes claims for us.

Uses and Disclosures of Protected Health Information Without Individual Authorization

Other Permitted Use and Disclosures PRUDENTIAL may make the following uses and disclosures of customer's information without customer's permission, in accordance with federal and state law:

- 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.
- To a law enforcement official for a law enforcement purpose.
- 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.

Required Uses and Disclosures

PRUDENTIAL must disclose your information when required by the Secretary of the Department of Health and Human Services to make sure PRUDENTIAL comply with federal law.

Uses And Disclosures That Will Only Be Made With Customer's Authorization

PRUDENTIAL will only make the following uses and disclosures with customer's written authorization:

- Uses and disclosures for marketing purposes;
- Uses and disclosures that constitute a sale of Protected Health Information;
- Most uses and disclosures of psychotherapy notes; and
- Other uses and disclosures not otherwise described in this Notice.

Customer may withdraw customer's authorization in writing at any time. To withdraw customer's authorization or if customer wish additional information. Once we receive customer's written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon your written authorization and prior to receiving customer's revocation. PRUDENTIAL may also continue to use and disclose your Protected Health Information after revocation if the authorization was obtained as a condition of securing insurance and other law provides us with the right to contest a claim under the policy or the policy itself.

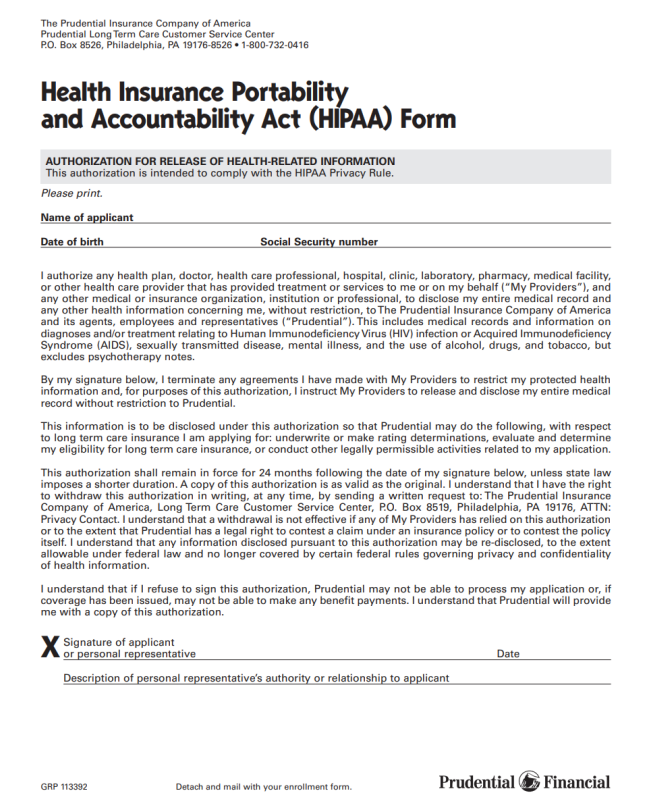
Individual Rights With Respect To Your Protected Health Information

- **RIGHT TO REQUEST RESTRICTIONS**: customer have the right to request in writing that restrictions be placed on certain uses and disclosures of customer's information. PRUDENTIAL are not required to agree. If PRUDENTIAL do agree,PRUDENTIAL we may not use or disclose any of customer's information except where customer need emergency treatment. PRUDENTIAL may end an agreement to restrict as allowed by federal law.
- **RIGHT TO ALTERNATIVE CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION**: If you choose to have customer's information sent to you by a means of customer's choice or to an address of customer's choice, PRUDENTIAL will do so if the request is reasonable. You must clearly state that disclosure of all or any part of customer's information could endanger customer if not sent per customer's choice. Any such request should be sent in writing to the contact listed at the end of this Notice.
- **RIGHT TO INSPECT AND COPY PROTECTED HEALTH INFORMATION**: customer have the right to inspect and copy customer's claims and other health information. All requests to exercise this right should be in writing and sent to the contact listed at the end of this Notice. PRUDENTIAL may deny customer's request in writing in certain very limited circumstances. If the information customer request is maintained electronically, and customer request an electronic copy, PRUDENTIAL will provide a copy in the electronic form and format customer request, if the information can be readily produced in that form and format. If the information cannot be readily produced in that form and format, PRUDENTIAL will work with customer to come to an agreement on form and format. PRUDENTIAL may charge a reasonable, cost-based fee. PRUDENTIAL are allowed by law to deny access in some cases, and subject to certain procedures. If customers are denied access, customer may request that the denial be reviewed by submitting a written request to the contact listed at the end of this Notice.
- **RIGHT TO AMEND PROTECTED HEALTH INFORMATION**: The customer have the right to request that PRUDENTIAL amend the customer's information kept in our records. PRUDENTIAL are allowed to deny customer's request in certain situations. For example, PRUDENTIAL may deny a customer's request if PRUDENTIAL did not create the information in the record. PRUDENTIAL will review the customer's request and respond to customer in writing. All requests should be in writing and sent to the contact listed at the end of this Notice. All requests should provide needed details, including the customer's name, address, insurance policy number, and the reason you think the customer's information needs to be changed.
- **RIGHT TO AN ACCOUNTING**: customer have the right to receive an accounting from us of disclosures of customer's information made for up to the six (6) years prior to customer's request. This right does not apply to certain disclosures, including the following: disclosures

made to carry out treatment, payment, or health care operations and certain other disclosures (such as any you authorized us to make). Any request should be sent to the contact listed at the end of this Notice. Your request must be made in writing and state the time period of the request, which may not be longer than six years prior to customer's request. The first request within a 12-month period will be provided to you free of charge, and any additional requests within this time period may be subject to a reasonable, cost-based fee. PRUDENTIAL will notify you prior to charging a fee, and you may choose to withdraw or modify customer's request at that time before any costs are incurred.

- **RIGHT TO A PAPER COPY OF THIS NOTICE**: customer have the right, even if you have agreed to receive notice by email, to get a paper copy of this Notice. All requests should be in writing and sent to the contact listed at the end of this Notice.
- **RIGHT TO FILE A COMPLAINT**: If you believe the customer's privacy rights have been violated, you have the right to complain to us by writing to the contact listed at the end of this Notice. customer may also send a complaint to the U.S. Department of Health and Human Services Office for Civil Rights, 200 Independence Avenue, S.W., Washington, DC 20201. Federal law prohibits retaliation or penalty against you for filing such a complaint. The contact listed at the end of this Notice is also available to provide you information regarding questions you have or other information concerning this Notice.

### 2.3.4 Sample Forms



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.

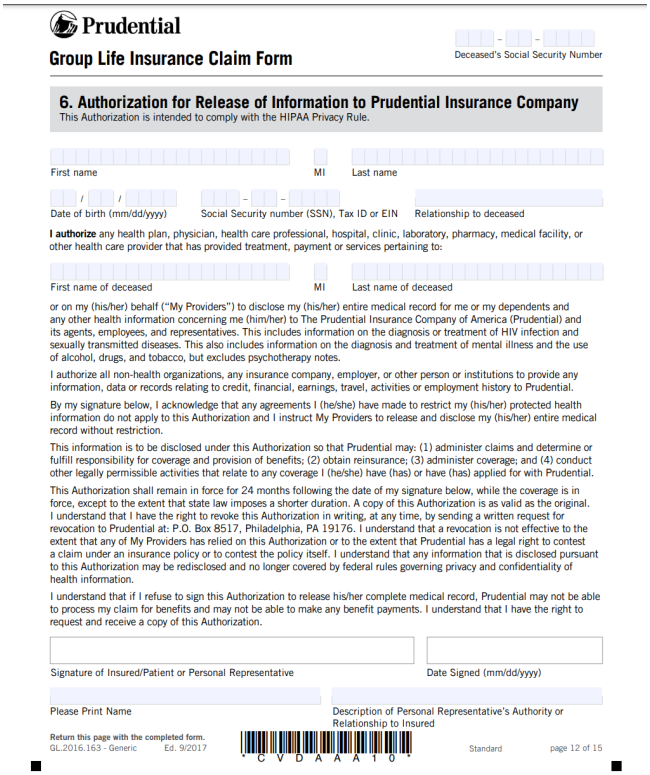
This authorization shall remain in force for 24 months following the date of my signature below, unless state law imposes a shorter duration. A copy of this authorization is as valid as the original. I understand that I have the right to withdraw this authorization in writing, at any time, by sending 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

**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

### 2.3.5 Example

Let's consider a scenario where a healthcare provider, such as a doctor or a hospital, needs to share a patient's medical records with Prudential Insurance Company of America, which provides Long-Term Care Insurance. The patient is seeking coverage and needs to provide their medical history for underwriting purposes. In this case, both the healthcare provider and Prudential must adhere to HIPAA regulations.

The healthcare provider must ensure that the patient's Protected Health Information (PHI) is kept private and disclose only the necessary information required for underwriting. They can share the patient's medical records securely, following HIPAA guidelines, to provide the necessary information for insurance coverage evaluation.

Prudential, as the insurance provider, must use the patient's medical information for underwriting purposes and determining the coverage and pricing. They can only use the patient's PHI as permitted by HIPAA, ensuring that it is not disclosed for any other unauthorized purposes.

Both parties should have safeguards in place to protect the confidentiality and security of the patient's medical information. They must also be prepared to provide the patient with access to their medical records, as required by HIPAA, and respect the patient's right to request restrictions on certain uses and disclosures of their information.

In summary, this example demonstrates how HIPAA regulations apply when a healthcare provider shares a patient's medical information with an insurance company for underwriting, ensuring the protection of the patient's privacy and compliance with HIPAA rules.

## 3 Conclusion

In 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 Training 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.

## 4 Reference

## References

[1] https://www.prudential.com/links/hipaa

[2] https://benefits.leidos.com/sites/benefits/files/2019-01/prudential-group-life-insurance-claim-form.pdf

[3] https://www.instantbenefits.com/sites/cust_ben/shoreline_sd/06-07/ltc_hipaa_form.pdf

[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-ron-tai-vinmec/

[8] https://www.pepperdine.edu/about/administration/provost/content/policies/hipaa-manual.pdf

[9] https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf