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

Content

Ref:	HIPAA Home | HHS.gov https://www.hhs.gov/hipaa/index.html
Problem statement	Khoa
Why it matters	Khoa
What it is	Khoa
How it works	Nguyên: focus on HIPAA for Individuals https://www.hhs.gov/hipaa/for-individuals/index.html Phong: focus on HIPAA for Professionals https://www.hhs.gov/hipaa/for-professionals/index.html
Application survey in Vietnam	Khoa

Problem statement ?

-The research will evaluate the effectiveness of the patient education and the implications of applying the HIPAA regulation privacy act on medical records. The general problem is that the patients and health staff have little knowledge concerning the privacy acts.

- As studies indicate, information control generally entails privacy. For over a decade concerns have been indicated on how hospitals unethically publicized information with sensitivity, improperly display of safeguarded health information and hence spoiling data control. The problem is that patients and Health staff were not in a position to understand the true implications of implementing the privacy regulations instead they only considered the minimum necessary requirement which is based on the real existing practice that confined wellbeing information ought not to be used or revealed when it is not needed

Why it matters?

- HIPAA is important because, due to the passage of the Health Insurance Portability and Accountability Act, the Department of Health and Human Services was able to develop standards that protect the privacy of individually identifiable health information and the confidentiality, integrity, and availability of electronic Protected Health Information.
- HIPAA was introduced in 1996, primarily to address one particular issue: Insurance coverage for individuals between jobs and with pre-existing conditions. Without HIPAA, employees faced a potential loss of insurance coverage between jobs. Because of the cost of HIPAA's primary objective to health insurance companies – and the risk that the cost would be passed onto employers and individuals as higher premiums, Congress instructed the Secretary for Health and Human Services to develop standards that would reduce healthcare insurance fraud and simplify the administration of healthcare transaction.

What it is?

-The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is legislation that is designed to make it easier for US workers to retain health insurance coverage when they change or lose their jobs.

- The legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing.

HIPAA for individuals

Learn your rights under HIPAA, how your information may be used or shared, and how to file a complaint if you think your rights were violated.

This includes information about their past, present, or future physical or mental health, the provision of health care to them, or the payment for health care to them.

What Information Is Protected ?

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer’s computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws

HIPAA also requires **covered entities** (the entities that must follow the HIPAA regulations):

- Health Plans
- Most Health Care Providers
- Health Care Clearinghouses

to take steps to protect the privacy of individuals' health information. This includes implementing safeguards to prevent unauthorized access, use, or disclosure of health information.

In addition, **business associates** of covered entities must follow parts of the HIPAA regulations.

Examples of business associates include:

- Companies that help your doctors get paid for providing health care, including billing companies and companies that process your health care claims
- Companies that help administer health plans
- People like outside lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

- Covered entities must have contracts in place with their business associates, ensuring that they use and disclose your health information properly and safeguard it appropriately.
- Business associates must also have similar contracts with subcontractors.
- Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule.

Who Is Not Required to Follow These Laws ?

Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

How This Information Is Protected ?

- Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.
- Business associates also must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.

HIPAA gives individuals a number of rights over their health information, including:

- Access and receive a copy of their health information.
- Provide corrections to their health records.
- Request that their health information not be disclosed to certain people or organizations.
- Learn about how their health information is being used and disclosed
- File a complaint with the Department of Health and Human Services if they believe their privacy rights have been violated.

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

The Privacy Rule sets rules and limits on who can look at and receive your health information

Personal information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it.

Example: Use or share your information for marketing or advertising purposes or sell your information.

Conclusion

- HIPAA is an important law that helps to protect the privacy of individuals' health information. By understanding their rights under HIPAA, individuals can take steps to ensure that their health information is protected.

- The purpose of HIPAA for individuals is to give them peace of mind knowing that their health information is protected. This can help individuals to be more open and honest with their health care providers, which can lead to better quality care. HIPAA can also help to prevent identity theft and fraud.

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

About HHS | Programs & Services | Grants & Contracts | Laws & Regulations

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

HHS > HIPAA Home

Health Information Privacy

I would like info on ...

- HIPAA and COVID-19
- HIPAA and Part 2
- New FTC-HHS Health App Tool
- Gender Affirming Care, Civil Rights, and Privacy - PDF
- Online Tracking Technologies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

HIPAA for Individuals
We offer information about your rights under HIPAA and answers to frequently asked questions about the HIPAA Rules.

Filing a HIPAA Complaint
You may file a complaint with O... feel your rights under the HIP... violated.

Other Languages

HIPAA for Professionals
Find information about the HIPAA Rules, guidance on compliance, OCR's enforcement activities, frequently asked questions, and more.

Newsroom
Read the latest HIPAA news ... and an archive of past releas...

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

HHS > HIPAA Home > HIPAA for Professionals

- HIPAA for Professionals
- Regulatory Initiatives
- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement +
- Special Topics +
- Patient Safety +
- Covered Entities & Business Associates +
- Training & Resources
- FAQs for Professionals
- Other Administrative Si...cation Rules

HIPAA for Professionals

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

-To improve the efficiency and effectiveness of the healthcare system.
-Required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.
-Congress recognized that advances in electronic technology could erode the privacy of health information.
-Privacy protections for individually identifiable health information.

HIPAA for Professionals

Definition of HIPAA for Professionals

Department of Health and Human Services ("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

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

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**.

The HIPAA Privacy Rule

The HIPAA Privacy Rule establishes **national standards to protect individuals' medical records and other individually identifiable health information** (collectively defined as “protected health information”) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

Click here to view the combined regulation text of all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164.

Summary of the HIPAA Privacy Rule

Who is Covered by the Privacy Rule

The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use CMS's decision tool.

Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. If an insurance entity has separable lines of business, one of which is a health plan, the HIPAA regulations apply to the entity with respect to the health plan line of business.

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.[7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

Business Associates

Business Associate Defined. In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.

Business Associate Contract. When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections).

HIPAA for Professionals

The HIPAA Privacy Rule

Health Plans

For HIPAA purposes, health plans include:

- Health insurance companies
- HMOs, or health maintenance organizations
- Employer-sponsored health plans
- Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs

Clearinghouses

Clearinghouses include organizations that process nonstandard health information to conform to standards for data content or format, or vice versa, on behalf of other organizations.

Providers

Providers who submit HIPAA transactions, like claims, electronically are covered. These providers include, but are not limited to:

- Doctors
- Clinics
- Psychologists
- Dentists
- Pharmacies
- Nursing homes
- Chiropractors

Summary of the HIPAA Privacy Rule

What Information is Protected

Protected Health Information. De-Identified Health Information.

Permitted Uses and Disclosures

(1) To the Individual.

(2) Treatment, Payment, Health Care Operations.

(3) Uses and Disclosures with Opportunity to Agree or Object.

(4) Incidental Use and Disclosure.

(5) Public Interest and Benefit Activities.

(6) Limited Data Set

HIPAA for Professionals

Summary of the HIPAA Privacy Rule

What Information is Protected: *Protected Health Information. *De-Identified Health Information.

Protected Health Information. The Privacy Rule protects all "***individually identifiable health information***" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Summary of the HIPAA Privacy Rule

What Information is Protected: *Protected Health Information. *De-Identified Health Information.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either:

(1) a formal determination by a qualified statistician;

or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]

HIPAA for Professionals

Summary of the HIPAA Privacy Rule

General Principle for Uses and Disclosures: A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization

(1) **To the Individual:** the individual who is the subject of the information.

(2) **Treatment, Payment, Health Care Operations:** for its own treatment, payment, and health care operations activities.

(3) **Uses and Disclosures with Opportunity to Agree or Object:** by asking the individual outright, or by circumstances

(4) **Incidental Use and Disclosure:** result of, or as "incident to," the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27]

(5) **Public Interest and Benefit Activities:** 12 national priority purposes. *Required by Law, Public Health Activities,...*

(6) **Limited Data Set:** certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed

Summary of the HIPAA Privacy Rule

Administrative Requirements:

Privacy Policies and Procedures.

Privacy Personnel.

Workforce Training and Management.

Mitigation.

Data Safeguards.

Complaints.

Retaliation and Waiver.

Documentation and Record Retention: 6 years

HIPAA for Professionals

Summary of the HIPAA Privacy Rule

Enforcement and Penalties for Noncompliance: ***Civil Money Penalties:** ***Criminal Penalties.**

Civil Money Penalties: Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

Penalty Amount Per Violation	$127 - $63,973* per violation
Calendar Year Cap for Violation of Identical Requirement or Prohibition	$25,000 - $1,919,173**

*The Department of Health and Human Services *may* make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. The annual inflation amounts are found at 45 CFR § 102.3.

**Pursuant to HHS's Notification of Enforcement Discretion, https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties

HIPAA for Professionals

Summary of the HIPAA Privacy Rule

Enforcement and Penalties for Noncompliance: ***Civil Money Penalties:** ***Criminal Penalties.**

Criminal Penalties.

- A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment.

-The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses,

- $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm.

The Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

View the combined regulation text of all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164.

HIPAA for Professionals

The Security Rule

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates.

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI ("electronic protected health information")
Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.[4]

The Security Rule

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.[6]

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.[7]

HIPAA for Professionals

The Security Rule

Risk Analysis and Management

Administrative Safeguards

- Security Management Process.
- Security Personnel.
- Information Access Management.
- Workforce Training and Management.
- Evaluation

Physical Safeguards

- Facility Access and Control.
- Workstation and Device Security.

Technical Safeguards

A covered entity must implement hardware, software, and/or procedural mechanisms and implement policies and procedures

- Access Control: only authorized persons.
- Audit Controls: record and examine access
- Integrity Controls: not improperly altered or destroyed.
- Transmission Security: against unauthorized access to e-PHI that is being transmitted over an electronic network.[27]

Enforcement and Penalties for Noncompliance: same as Privacy Rule

Application survey in Vietnam

-Trong luật khám chữa bệnh Việt Nam (điều 8, mục 1, chương II) quy định bệnh nhân được quyền giữ bí mật thông tin về tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án.

Điều 8. Quyền được tôn trọng bí mật riêng tư:

1. Được giữ bí mật thông tin về tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án.

2. Thông tin quy định tại khoản 1 Điều này chỉ được phép công bố khi người bệnh đồng ý hoặc để chia sẻ thông tin, kinh nghiệm nhằm nâng cao chất lượng chẩn đoán, chăm sóc, điều trị người bệnh giữa những người hành nghề trong nhóm trực tiếp điều trị cho người bệnh hoặc trong trường hợp khác được pháp luật quy định.

Điều 59. Hồ sơ bệnh án

3. Việc lưu trữ hồ sơ bệnh án được quy định như sau:

a) Hồ sơ bệnh án được lưu trữ theo các cấp độ mật của pháp luật về bảo vệ bí mật nhà nước;

Application survey in Vietnam

5. Các đối tượng quy định tại khoản 4 Điều này khi sử dụng thông tin trong hồ sơ bệnh án phải giữ bí mật và chỉ được sử dụng đúng mục đích như đã đề nghị với người đứng đầu cơ sở khám bệnh, chữa bệnh.

Một vài ví dụ:

- Một vài cơ sở khám chữa bệnh đã áp dụng HIPAA để bảo vệ dữ liệu thông tin cá nhân của người bệnh như “doctor có sẵn” (https://www.docosan.com/chinh-sach-bao-ve-thong-tin-ca-nhan)

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

Cảm ơn thầy và cả lớp đã theo dõi.