HIPAA WORKFORCE TRAINING

HIPAA AND CONSUMER PRIVACY
HIPAA HISTORICAL BACKGROUND

• The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress and signed by President Bill Clinton in 1996.

• This law was enacted as part of a broad congressional attempt at incremental healthcare reform.
HIPAA: BROKEN DOWN

• **TITLE 1**: Protects health insurance coverage for workers and their families when they change or lose their jobs.

• **TITLE 3**: Provides for certain tax deductions for medical insurance, and makes other changes to health insurance law.

• **TITLE 4**: Specifies conditions for group health plans regarding coverage of persons with pre-existing conditions, and modifies continuation of coverage requirements.

• **TITLE 5**: Includes provisions related to company-owned life insurance, treatment of individuals who lose U.S. Citizenship for income tax purposes, and prohibits the tax-deduction of interest on life insurance loans, company endowments, or contracts related to a financial institution.
Title II: HIPAA Administrative Simplification

• Requires the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

• Adopting these standards have dramatically improved the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

• **Addresses the security and privacy of health data.**
HIPAA
Health Insurance and Portability Act of 1996

Title I
Portability

Title II
Administrative Simplification

Title III
Medical Savings Accounts

Title IV
Group Health Plan Provisions

Title V
Revenue Offset Provision

PRIVACY
Use and Disclosure of PHI
Individual Rights
Administrative Requirements

EDI
Transactions
Code Sets
Identifiers

SECURITY
Administrative Procedures
Physical Safeguards
Technical Security Services
Technical Security Mechanisms
What is Protected Health Information (PHI)?

- PHI is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
- Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by the health provider, (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (3) identifies the individual.
Examples of PHI

- Names
- Geographical identifiers
- Dates directly related to an individual
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Any medical information obtained from an individual’s medical record.
The HIPAA Security Rule

• The HIPAA Security Rule establishes national standards to protect individuals’ electronic PHI 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 PHI.
Why Security?

- Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry.
- At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of computers to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.
- While this means that the medical workforce can be more mobile and efficient, the rise in the adoption rate of these technologies creates an increase in security risks.
Security Standards

• The security standards are designed to be “technology neutral” to accommodate changes.
• The rule does not prescribe the use of specific technologies, so that the health care community will not be bound by specific systems and/or software that may become obsolete.
• The rule also recognizes that the security needs of health care entities can vary significantly. This flexibility within the rule enables each entity to choose technologies to best meet its specific needs and comply with the standards.

• The security standards are divided into the categories of administrative, physical, and technical safeguards.
Administrative Safeguards

• In general, these are the administrative functions that should be implemented to meet the security standards.

• Administrative safeguards include:
  o Assignment or delegation of security responsibility to an individual(s)
  o Security training requirements
  o Workforce security
  o Information access management
  o Business Associate Contracts

45 C.F.R. §164.308
Physical Safeguards

• In general, these are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion.

• Physical Safeguards include:
  o Restricting access to EPHI
  o Retaining off site computer backups.
  o Workstation security
  o Device and media controls

45 C.F.R. § 164.310
Technical Safeguards

• In general, these are primarily the automated processes used to protect data and control access to data.

• Technical safeguards include:
  o Using authentication controls to verify that the person signing onto a computer is authorized to access the EPHI.
  o Transmission controls, such as encrypting and decrypting data as it is being stored and/or transmitted.
  o Audit controls.

45 C.F.R. § 164.312
The HIPAA Privacy Rule

• The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal 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 personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

• The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
Privacy Rule vs. Security Rule

• The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to PHI will actually have access.

• The Privacy Rule also applies to all forms of patients’ PHI, whether electronic, written, or oral. In contrast, the Security Rule covers only protected health information that is in electronic form. This includes EPHI that is created, received, maintained or transmitted. For example, EPHI may be transmitted over the Internet, stored on a computer, a CD, a disk, magnetic tape, or other related means.
Important Definitions in the Privacy Rule

• **Covered Entity:**
  o A health plan.
  o A health care clearinghouse.
  o A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

• **Business Associate:**
  o An entity that creates, receives, maintains, or transmits protected health information on behalf of a covered entity.
  o Includes claims processing or administration, data analysis, processing, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

• **Subcontractor:**
  o A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
Uses and Disclosures of PHI

• A covered entity or business associate may not use or disclose protected health information, except as permitted or required.
Required Uses and Disclosures

• To an individual

• When required by the Secretary of HHS to investigate the entity's HIPAA compliance

• Business Associates: To a covered entity as necessary to satisfy a covered entity's obligations
1. For treatment, payment, or health care operations

- A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

- A covered entity may disclose protected health information for treatment activities of a health care provider.

- A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
Permitted Uses and Disclosures

2. Pursuant to a valid authorization
   o Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without a valid authorization.
   o When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization

45 C.F.R. § 164.508
Permitted Uses and Disclosures

Instances where an authorization is always required:

- **Psychotherapy notes** – A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
  - To carry out the following treatment, payment, or health care operations:
    - Use by the originator of the psychotherapy notes for treatment
    - Use or disclosure by the covered entity for its own training programs
    - Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual.

- Marketing
- Sale of PHI

45 C.F.R. § 164.508
Permitted Uses and Disclosures

Required Contents of an Authorization:

• A description of the information to be used or disclosed that specifically identifies the information.
• The name of the person authorized to make the requested use or disclosure.
• Identify the person(s) or entity to whom the covered entity may make the requested use or disclosure.
• A description of each purpose of the requested use or disclosure.
• An expiration date or an expiration event.
• Signature of the individual or the individual’s personal representative, and date.

45 C.F.R. § 164.508
Permitted Uses and Disclosures

In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

• The individual's right to revoke the authorization in writing
• The inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization
• The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient

45 C.F.R. § 164.508
3. Situations where the patient has the opportunity to agree or object (not requiring written authorization)

- Facility directories
- A covered entity may disclose to a family member or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment.
- If the individual is not present or is incapacitated, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual, and disclose only the PHI that is directly relevant.
Permitted Uses and Disclosures

4. Uses and disclosures not requiring authorization or an opportunity to agree or object

- Uses and disclosures required by law
  - Disclosures about individuals reasonably believed to be victims of abuse, neglect or domestic violence.
  - Uses and disclosures for health oversight activities.
  - Disclosures for judicial and administrative proceedings.

- Uses and disclosures for public health activities
- Uses and disclosures for law enforcement purposes
- Uses and disclosures for workers compensation

45 C.F.R. § 164.510
Minimum Necessary Standard

- A covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- Does not apply for:
  - Disclosures to or requests by a health care provider for treatment
  - Uses or disclosures made to the individual
  - Uses or disclosures made pursuant to an authorization
  - Disclosures made to the Secretary
  - Uses or disclosures that are required by law
  - Uses or disclosures that are required for compliance with HIPAA

45 C.F.R. § 164.502
De-identification of PHI

• Health information that does not identify an individual, and cannot be used to identify an individual, is not individually identifiable health information, and is therefore not PHI
• Requires removal of the following identifiers:
  o Names
  o Geographic subdivisions smaller than State
  o Dates
  o Telephone numbers
  o Fax numbers
  o Email addresses
  o Social security numbers
  o Medical record numbers
  o Health plan beneficiary numbers
  o Account numbers
  o Certificate/license numbers
  o Vehicle identifiers and serial numbers
  o Device identifiers and serial numbers
  o URLs
  o IP address numbers
  o Biometric identifiers, including finger/voice prints
  o Full face photographic images

45 C.F.R. § 164.514
Notice of Privacy Practices

An individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

PATIENT INFORMATION

Notice of Privacy Practices

45 C.F.R. § 164.520
Implementing the Privacy Rule

A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

A covered entity must train all members of its workforce on the policies and procedures with respect to PHI.

A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

45 C.F.R. § 164.530
Implementing the Privacy Rule

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures.

A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity.

A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of any right or for participation in any process, including the filing of a HIPAA complaint.

45 C.F.R. § 164.530
The Relationship Between Covered Entities, Business Associates, and Subcontractors
Business Associate Agreements

• A covered entity may permit a business associate to create, receive, maintain, or transmit PHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

• A business associate may permit a subcontractor to create, receive, maintain, or transmit PHI on its behalf only if the business associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information.

• “Satisfactory assurances” are obtained through the use of a Business Associate Agreement.

45 C.F.R. § 164.308
Contents of Business Associate Agreements

• The contract must provide that the business associate will:
  o Comply with the applicable requirements of HIPAA;
  o Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to comply with the applicable HIPAA requirements by entering into a contract or other arrangement; and
  o Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI.

45 C.F.R. §164.314
Contents of Business Associate Agreements

• Other provisions that should be included:
  o Obligations and activities of business associate
  o Permitted uses and disclosures by business associate
  o Requirement that covered entity must inform business associate of privacy practices and restrictions
  o Permissible requests by covered entity
  o Term and termination
  o How and when notification of security incidents by the business associate must be provided to the covered entity

• Model Business Associate Agreement provided at http://www.hhs.gov/ocr/privacy
Covered Entity and Business Associate HIPAA Liability

• Covered entities and business associates are separately and directly liable for violation of applicable provisions of the Security and Privacy Rules.
• Previously, business associates were only contractually liable to a covered entity pursuant to the terms of a business associate agreement.
• Business associates must ensure that any subcontractors that use PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information.
• If a subcontractor violates the terms and conditions of HIPAA or the business associate agreement, they may be held contractually liable to the business associate.
Recent Changes

• Prior to 2013, covered entities could not be held liable for their business associates’ HIPAA violations if the covered entity had an appropriate business associate agreement in place and either did not know of the business associate’s material breach of the agreement, or took reasonable steps to cure the breach and terminated the agreement or reported the problem to HHS if such steps were unsuccessful.

• In 2013, this safe harbor was removed. A covered entity can now be held liable for the acts or omissions of its business associates that are acting as the covered entity’s “agent.” This agency liability also extends to a business associate for the actions or omissions of its subcontractors.
What is an Agent?

HHS has indicated that the essential factor in determining whether an agency relationship exists is the right or authority of a covered entity to control the business associate’s conduct in the course of performing a service on behalf of the covered entity.
What is an Agent?

• A number of other factors must also be considered:
  o The time, place and purpose of the business associate’s conduct;
  o Whether the business associate engaged in a course of conduct subject to the covered entity’s control;
  o Whether services provided by the business associate are commonly performed by business associates on behalf of covered entities; and
  o Whether or not the covered entity would reasonably expect the business associate to engage in the conduct in question.

• Ultimately, the more discretion and independence the business associate has in performing functions for the covered entity, the less likely it is that an agency relationship exists.
HIPAA BREACHES
How to Identify and Respond to Breach Situations
What is a Breach?

Breach means the acquisition, access, use, or disclosure of protected health information in a manner **not permitted**, which **compromises** the security or privacy of the protected health information.

45 C.F.R. §164.402
What is a Breach?

Three situations excluded as a breach:

• Any unintentional acquisition, access, or use of PHI by a workforce member of a covered entity or a business associate, if it was made in good faith and within the scope of authority and does not result in further use or disclosure

• Any inadvertent disclosure to another person authorized to access PHI at the same covered entity or business associate, and the information received as a result of such disclosure is not further used or disclosed

• A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

45 C.F.R. §164.402
What is a Breach?

An acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

45 C.F.R. § 164.402
Breach Assessment

First Factor: The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

Consider:

- Whether the disclosure involved information that is of a sensitive nature
- The amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results)
- Whether the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient’s own interests
- If there are few direct identifiers in the information impermissibly used or disclosed, whether there is a likelihood that the PHI released could be re-identified

45 C.F.R. §164.402
Breach Assessment

Second Factor: The unauthorized person who used the PHI or to whom the disclosure was made.

- Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information.
- For example, if PHI is impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.

45 C.F.R. §164.402
Breach Assessment

Third Factor: Whether the PHI was actually acquired or viewed.

Examples:
If a covered entity mailed information to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.

Encryption
• If PHI is secured by encryption, rendering it unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS

45 C.F.R. §164.402
Breach Assessment

Fourth Factor: The extent to which the risk to the PHI has been mitigated.

• Entities should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, including:
  o Obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed, or will be returned or destroyed
  o Notification letters to affected individuals
  o Credit monitoring protection
  o Re-training
  o Discipline and sanctions
  o Review of HIPAA policies

• Entities should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised

45 C.F.R. §164.402
Breach Assessment

• If after analyzing these factors in a risk assessment, the entity can demonstrate that there is a low probability that the PHI has been compromised, there is no breach.

• However, if the entity cannot demonstrate that there is a low probability that the PHI has been compromised, the presumption remains that there is a breach.
Breach Obligation: Notification

Business Associates:
• Must notify the covered entity within 60 days of the discovery of the breach

Covered Entities:
• Must notify the affected individuals in writing within 60 days of the discovery of the breach
  o If deceased, next of kin must be notified
  o If no contact information, substitute notice must be provided
• Must notify the Office for Civil Rights (OCR)
  o If more than 500 individuals affected by the breach, within 60 days
  o If less than 500 individuals affected by the breach, within 60 days of the end of the calendar year
• Must notify the media if more than 500 individuals affected by the breach

45 C.F.R. §§ 164.404; 164.406; 164.408; 164.410
OCR Breach Investigations

Major Sources of HIPAA Breach Investigations:
- Complaints
- OCR notification reports
- Compliance reviews

The issues investigated most are:
- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
- Lack of patient access to their PHI
- Uses or disclosures of more than the minimum necessary PHI
- Lack of administrative safeguards of electronic PHI
If an investigation ensues, OCR will notify the person who filed the complaint and the covered entity named in it. Then the complainant and the covered entity are asked to present information about the incident or problem described in the complaint. OCR may request specific information from each to get an understanding of the facts.

Covered entities are required by law to cooperate with complaint investigations.
If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement

If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties on the covered entity.

If monetary penalties are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.

Complainants do not receive a portion of monetary penalties collected from covered entities.
## Potential Penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
California Confidentiality of Medical Information Act

Significant overlap between HIPAA and CMIA

One major difference: there is no private right to sue under HIPAA, while an individual can sue for violation of their privacy rights under the CMIA.

A patient whose medical information has been used or disclosed in violation of CMIA and who has sustained economic loss or personal injury, may file a lawsuit and recover compensatory damages, punitive damages up to $3,000, attorneys' fees up to $1,000, and the costs of litigation.

Cal. Civ. Code § 56.36