

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview

First **1** 2 3 4 5 6 Next Page » Last



## Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules

Includes updates from the Final Omnibus Rule

Effective April 14, 2003; Updated January 23, 2013



Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview

First « Previous Page 1 **2** 3 4 5 6 Next Page » Last

### Course Overview

#### Purpose of Course

- A self-study educational module to ensure your knowledge of HIPAA and your responsibility to comply.
- This training module includes important information from the Omnibus Final Rule updates to the HIPAA 1996 Privacy and Security Rules.

#### Course Objective

- Understand HIPAA (Health Insurance Portability and Accountability Act) rules and regulations.
- Understand your responsibilities as a Healthcare Industry Representative (HCIR) when interacting with healthcare professionals.



Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview

First « Previous Page 1 2 3 4 5 6 Next Page » Last

### Introduction

#### Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Effective April 14, 2003; Updated January 23, 2013.

#### Key elements of HIPAA:

- The Privacy Rule established national standards for protection of certain health information.
- The Rule addresses the use and disclosure of individuals' health information, called protected health information (PHI) by covered entities (CE) --as well as standards for the rights of individuals to understand and control how their health information is used.
- Security Rule establishes a national set of standards for protecting certain health information that is held or transferred in electronic form, essentially addresses the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).
- Within HHS, the Office for Civil Rights (OCR) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

EXIT

**HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview**

First « Previous Page 1 2 3 **4** 5 6 Next Page » Last

## HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

## Health Care Description

### Covered Entities (CE):

- Doctors, clinics, hospitals, dentists, nursing homes, and pharmacies that transmit data electronically
- Health plans (small plans as of 2004)
- Healthcare clearinghouses

### Business Associates (BA):

- Any person or organization that functions on behalf of a covered entity that involves use or disclosure of identifiable health information.

- |                         |                      |                        |
|-------------------------|----------------------|------------------------|
| ▪ External labs         | ▪ Documentation      | ▪ Clearinghouses       |
| ▪ Claims processing     | ▪ Data processing    | ▪ Transcriptionists    |
| ▪ CPA firms             | ▪ Insurers           | ▪ Facilities managers  |
| ▪ External auditors     | ▪ Network/server     | ▪ Pharmacies           |
| ▪ Translators           | ▪ Software companies | ▪ Benefit manager      |
| ▪ Answering services    | ▪ 3rd party IT       | ▪ Accreditation orgs   |
| ▪ Coding auditors       | ▪ E-prescribers      | ▪ Benefit manager      |
| ▪ 3rd party call center | ▪ Attorneys          | ▪ Re-pricing           |
| ▪ Shredding             | ▪ Consultants        | ▪ Utilization reviewer |

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview

First « Previous Page 1 2 3 4 **5** 6 Next Page » Last

## Health Care Description

### Protected Health Information (PHI):

The Privacy Rule protects all "individually identifiable health information" (IIHI) 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)."

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

EXIT

**HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Introduction and Overview**

First « Previous Page 1 2 3 4 5 **6** Last

## HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

## Health Care Description

### Electronic Media:

- Electronic storage material where data is stored or recorded electronically.
  - ✓ Examples: computers, jump drives, digital memory.

### Genetic Information:

- GINA amendments define genetic information to mean information about the "genetic tests" of an individual, the genetic tests of an individual's "family members" and information about the "manifestation" of a disease or disorder of an individual's family members (i.e., family medical history). Genetic information also includes information about any request for, or receipt of, "genetic services," as well as information about any participation in clinical research that includes genetic services.

### Breach:

- Situations where there is an impermissible use or disclosure of protected health information that creates a risk of harm to patients. It could be financial harm, or reputational harm, because very personal details about those individuals are now exposed.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First **1** 2 3 4 5 6 7 8 9 10 Next Page » Last

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

# Complying with HIPAA Privacy and Security Rules

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

EXIT

**HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement**

First « Previous Page 1 **2** 3 4 5 6 7 8 9 10 Next Page » Last

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

## Protected Health Information (PHI)

**Under HIPAA “Individually identified 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 an individual
- The past, present, or future payment for the provision of health care to the individual
- Identifies the individual or is information for which there is a reasonable basis to believe it can be used to identify the individual.

**Protected health information can be in any form -- electronic, paper or oral. It can include financial and demographic information collected from patients.**

- Examples: Name, Address, Birth Date, Social Security Number



Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 1 2 **3** 4 5 6 7 8 9 10 Next Page » Last

### Covered Entities (CE's) and Business Associates (BA's)

- When a CE uses a contractor or other non-workforce member to perform "business associate" services or activities, the CE must have an agreement in place to include specified written safeguards for the PHI used or disclosed by the BA and the BA's contractors.
- BA's and their contractors are directly liable for compliance with certain provisions of the HIPAA rules
- A covered entity may disclose PHI about an FDA regulated product to manufacturers for reasons related to quality, safety, or effectiveness.
- Examples:
  - ✓ Adverse event reporting
  - ✓ Product tracking concerns
  - ✓ Product recalls
  - ✓ Post marketing surveillance

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 1 2 3 **4** 5 6 7 8 9 10 Next Page » Last

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

## Business Associates

A business associate functions or activities on behalf of a CE that involve the use of PHI or performs services to a CE:

- Claims processing
- Data analysis
- Utilization review
- Billing
- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation
- Management/administrative
- Accreditation,
- 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.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 1 2 3 4 **5** 6 7 8 9 10 Next Page » Last

### Business Associates

- BA's must agree to terms of a BA agreement with a CE where there will be use and disclosure of PHI.
- BA's must make reasonable effort to limit PHI access to the "minimum necessary" in order to accomplish the required activity.
- BA's and their contractors are contractually obligated by a Business Associate Agreement (BAA) and are directly liable for compliance with certain provisions of the HIPAA rules.
- It is the BA's responsibility have a BA agreement with all subcontractors that create or received PHI on their behalf.
- If asked by a covered entity to sign a BAA, HCIR's should consult their company's legal department first.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 1 2 3 4 5 **6** 7 8 9 10 Next Page » Last

### PHI can be De-Identified

- The privacy rule permits a CE or its business associate to de-identify PHI. A CE or their BA can create information for secondary use in comparative studies, policy assessment, and life science research that is not individually identifiable by following its de-identification standards.
- De-identification mitigates privacy risks by removing health data that individually identifies the individual and with respect to which there is no reasonable basis to believe that the information can be used to identify the individual.
- **De-identification occurs either by:**
  - (1) Safe Harbor in removing 18 identifiers and verifying there is no actual knowledge that the residual information can be identify the individual; **or**
  - (2) Expert has documented its statistical or scientific analysis determining that there is a very small risk of an anticipated recipient using such health information with other reasonably available information to identify an individual who is a subject of the information.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 2 3 4 5 6 **7** 8 9 10 Next Page » Last

## Breach Enforcement, Penalties and Notification Rules

Welcome **MICHAEL MCKAY**

View Test Status ▶

View Certificate ▶

Course Map ▶

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

◀ Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 3 4 5 6 7 **8** 9 10 Next Page » Last

## Business Enforcement and Penalties 4 Categories

The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing the Privacy standards and may conduct complaint investigations and compliance reviews.

VIOLATION TYPE	EACH VIOLATION	REPEAT VIOLATIONS/YR
Did Not Know	\$100 – \$50,000	\$1,500,000
Reasonable Cause	\$1,000 – \$50,000	\$1,500,000
Willful Neglect – Corrected	\$10,000 – \$50,000	\$1,500,000
Willful Neglect – Not Corrected	\$50,000	\$1,500,000

One-time violations stay under \$50k, but repeat violations within the same year can hold a fine of \$1.5 million across all HIPAA violation categories, *up substantially from the previous \$250k minimum.*

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

#### HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 4 5 6 7 8 9 10 Next Page » Last

### Covered Entities (CE's) and Business Associates (BA's)

- When a CE uses a contractor or other non-workforce member to perform "business associate" services or activities, the CE must have an agreement in place to include specified written safeguards for the PHI used or disclosed by the BA and the BA's contractors.
- BA's and their contractors are directly liable for compliance with certain provisions of the HIPAA rules
- A covered entity may disclose PHI about an FDA regulated product to manufacturers for reasons related to quality, safety, or effectiveness.
- Examples:
  - ✓ Adverse event reporting
  - ✓ Product tracking concerns
  - ✓ Product recalls
  - ✓ Post marketing surveillance

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Compliance and Breach Enforcement

First « Previous Page 5 6 7 8 9 **10** Last

## Incidental Use or Disclosure

The Privacy Rule permits certain **incidental uses and disclosures** that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure.

**An incidental disclosure is one that:**

- Cannot reasonably be prevented
- Is limited in nature
- Occurs as a by-product of an otherwise permitted use or disclosure

### **Example:**

Sign-in sheets or Physician's talking to patients in semi-private rooms

However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.



Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First **1** 2 3 4 5 6 7 Next Page » Last

# HIPAA Privacy Rule - Marketing

Welcome **MICHAEL MCKAY**

View Test Status ▶

View Certificate ▶

Course Map ▶

HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

◀ Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 1 **2** 3 4 5 6 7 Next Page » Last

## HIPAA Privacy Rule - Marketing

- The Privacy Rule defines “marketing” as making “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.”
- The Rule distinguishes marketing communications from those communications about goods and services that are essential for quality health care.
- How the Rule Works – The Privacy Rule addresses the use and disclosure of protected health information for marketing purposes by:
  - Defining what is “marketing” under the Rule;
  - Excepting from that definition certain treatment or health care operations activities;
  - Requiring individual authorization for all uses or disclosures of protected health information for marketing purposes with limited exceptions.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 1 2 3 4 5 6 7 Next Page » Last

## HIPAA Privacy Rule - Marketing

A CE may not sell protected health information to a BA or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

### Examples of Marketing

- A health plan sells a list of its members to a company that sells blood glucose monitors, which intends to send the plan's members brochures on the benefits of purchasing and using the monitors.
- A drug manufacturer receives a list of patients from a covered health care provider and provides remuneration, then uses that list to send discount coupon for a new anti-depressant medication directly to the patients.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 1 2 3 4 5 6 7 Next Page » Last

## HIPAA Privacy Rule - Marketing

- To determine what constitutes an acceptable “authorization,” see 45 CFR 164.508. If the marketing involves direct or indirect remuneration to the CE from a third party, the authorization must state that such remuneration is involved. See 45 CFR 164.508(a)(3).
- A communication does not require an authorization, even if it is marketing, if it is in the form of a face-to-face communication made by a CE to an individual; or a promotional gift of nominal value provided by the CE.
- **For example, no prior authorization is necessary when:**
  - A hospital provides a free package of formula and other baby products to new mother as they leave the maternity ward.
  - An insurance agents sells a health insurance policy in person to a customer and proceeds to also market a casualty and life insurance policy as well.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 1 2 3 4 **5** 6 7 Next Page » Last

## HIPAA Privacy Rule – Marketing Summary

- A covered entity cannot share PHI without written authorization from the person whose information is being shared.
- A Health Professional cannot give you a list of patients for distributing marketing materials or coupons.
- Marketing and product promotion are where companies are most vulnerable to improperly disclosing PHI.
- Never ask the names or other protected health information of patients.

Welcome **MICHAEL MCKAY**

[View Test Status](#) ▶

[View Certificate](#) ▶

[Course Map](#) ▶

**HIPAA Introduction and Overview**

**HIPAA Compliance and Breach Enforcement**

HIPAA Privacy Rule

Questions

◀ [Back To My Account](#)

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 1 2 3 4 5 **6** 7 Next Page » Last

## HIPAA Privacy Rule-Patient Consents and Authorizations

- Covered entities do not need a patient's consent to use or disclose PHI for treatment, payment, or healthcare operations.
- Patient authorization is required by HIPAA for the use and disclosure of PHI not related to treatment, payment, or healthcare operations.
- HCP's must obtain written authorization before sharing PHI with Pharmaceutical representative.

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach  
Enforcement

HIPAA Privacy Rule

Questions

Back To My Account

EXIT

HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> HIPAA Privacy Rule

First « Previous Page 2 3 4 5 6 **7** Last

## HIPAA Privacy Rule – Valid Authorizations

- Patient Authorizations to use PHI must include.
  - How the information is to be used or disclosed. For example: “Share specific types of PHI with Company X for the purpose of Z”
  - The right to revoke authorization
  - An expiration date

Welcome **MICHAEL MCKAY**

View Test Status

View Certificate

Course Map

HIPAA Introduction and Overview

HIPAA Compliance and Breach Enforcement

HIPAA Privacy Rule

Questions



Back To My Account

EXIT

## HIPAA Privacy and Security Rules Includes updates from the Final Omnibus Rule >> Questions

Please answer the questions below to complete this course.

**Q.1. The Privacy Rule sets the standards for the rights of individuals to understand and control how their health information is used.**

- ☐ True
- ☐ False

**Q.2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was updated January of 2013 as part of the final Omnibus Rule.**

- ☐ True
- ☐ False

**Q.3. The HIPAA definition of PHI is which of the following?**

- ☐ Public Health Information
- ☐ Protected Health Information
- ☐ Processed Health Information

**Q.4. Which accurately describes types of covered entities (CEs):**

- ☐ Doctors, clinics, hospitals, dentists, nursing homes, and pharmacies that transmit data electronically
- ☐ Doctors, clinics, hospitals, dentists, nursing homes, and pharmacies
- ☐ Doctors, clinics, hospitals, dentists, healthcare delivery services, and pharmacies

**Q.5. BA's and their contractors are directly liable for compliance with certain provisions of the HIPAA rules.**

- ☐ True
- ☐ False

**Q.6. Within HHS, the Office for Civil Rights (OCR) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.**

- ☐ True
- ☐ False



**Q.7. A healthcare covered entity (CE) is which of the following:**

- ☐ Healthcare Provider
- ☐ Health Plan
- ☐ Healthcare Clearinghouse
- ☐ All Listed

**Q.8. BA's and their contractors are contractually obligated by a Business Associate Agreement (BAA) and are directly liable for compliance with certain provisions of the HIPAA rules.**

- ☐ True
- ☐ False

**Q.9. PHI can be in any form or media whether electronic, paper, or oral?**

- ☐ True
- ☐ False

**Q.10. A BA is any person or organization that functions on behalf of a covered entity (CE) that involves use or disclosure of identifiable health information.**

- ☐ True
- ☐ False

**Q.11. There are three acceptable methods for de-identification?**

- ☐ True
- ☐ False

**Q.12. A patient's room number is an example of an incidental use or disclosure examples.**

- ☐ True
- ☐ False

**Q.13. You are permitted to receive a patient list from a healthcare professional to distribute marketing materials or coupons?**

- ☐ True
- ☐ False

**Q.14. Patient authorization is required by HIPAA for the use and disclosure of PHI not related to treatment, payment, or healthcare operations.**

- ☐ True
- ☐ False

**Q.15. To ensure the security ePHI, HIPAA recommends which of the of the following:**

- ☐ Keep a dedicated terminal open to any employee who has signed a confidentiality agreement to monitor.
- ☐ Password protect all laptops, electronic devices and computers where ePHI is stored.
- ☐ Ask another employee to save your data and protect it for you.

submit