



**PREMIER**  
SENIOR MARKETING, INC.

# HIPAA Overview

Health Insurance Portability and Accountability Act

Premier Senior Marketing, Inc

---



# HIPAA Defined

- Acronym that stands for the Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule. HIPAA took effect on April 14, 2003.
-



# Definitions

• **Authorization**: a patient consent or permission form clearly defined in HIPAA law that allows a covered entity to disclose Protected Health Information (PHI)

• **Disclose**: give out or release PHI; can be lawful or unlawful

• **Business Associate (BA)**: (us) person or company not part of covered entity's workforce, but works and uses medical and patient info; the ARRA made BA's a regulated entity under HIPAA law.

• **Protected Health Information: (PHI)** this is what HIPAA protects, includes medical records and billing records.

• **Covered Entity (CE)**: entities covered by HIPAA law, must comply with HIPAA. Medical Providers, Health Plans, and Clearing Houses are the 3 types.

• **American Recovery and Reinvestment Act (ARRA) and HiTech Act**: (Feb 18, 2010) Expanded and modified HIPAA; the ARRA made BA's (us) a regulated entity under HIPAA law. The HiTech Act made rules and regulations pertaining to electronic PHI (ePHI).

• **Minimum Necessary Rule (MNR)**: only the minimum necessary amount of PHI should be used

• **Electronic PHI**: (ePHI) electronic forms of PHI



## Effects of the American Recovery and Reinvestment (ARRA) and Hi-Tech Acts

- Tougher enforcement of HIPAA regulations, higher fines for violations
  - Mandatory investigations and fines for willful neglect
  - Affected people **MUST** be notified of the breach regarding their PHI
  - Added Business Associates (us) as a regulated entity under HIPAA law
  - Made laws and regulations pertaining to ePHI
-



## 5 Objectives of HIPAA

1. Make Health Insurance affordable and easier to change (i.e. easier to change when changing jobs)
  2. Prevent/Reduce Health Care fraud
  3. Improve efficiency and effectiveness of Healthcare transactions (i.e. insurance claims)
  4. Protect personal/confidential medical info, with mandatory privacy and security safeguards
  5. Gather statistical data to protect the population against disease
-



## 2 Primary Reasons HIPAA Exists

- To Protect Medical Privacy
- To Prevent Crime



## 2 Most Important HIPAA Rules

### Privacy Rule

- A set of national standards for the protection of health information
- Addresses the use and disclosure of individuals' Protected Health Information (PHI)

### Security Rule

- A set of national standards for the protection of ELECTRONIC forms of protected health information
  - Addresses the use and disclosure of individuals' electronic Protected Health Information (ePHI)
-



# Tips for Protecting ePHI

- Never Access ePHI unless authorized to do so
  - Use strong passwords, phrases, and timed screensavers
  - Never access computers under someone else's password
  - Don't leave PHI or ePHI files open
  - Use encryption for emailing ePHI, or DON'T email it
  - Properly lock, store, and dispose of PHI and ePHI
  - Be aware of hackers, scammers impersonating authorized personnel
  - Verify identities before giving out ePHI
-



**PREMIER**  
SENIOR MARKETING, INC.

# Fines for Violations

There is a minimum \$100 fine per violation  
per person,

With a maximum fine of \$50,000 per  
violation per person, and a **\$1.5 million**  
yearly cap

---



**PREMIER**  
SENIOR MARKETING, INC.

# Examples of HIPAA Violations

The business associate **incorrectly updated the contract holders' addresses resulting in the mailing of protected health information to incorrect recipients.** The breach affected approximately 3,400 members. The protected health information involved included demographic information, EOBs, clinical information, and diagnoses. In response to this incident, the covered entity took steps to enforce the requirements of its business associate agreement with SBP. The business associate improved its code review process to catch the system error that caused this incident and instituted a manual quality review process designed to identify bad addresses.

The covered **entity inadvertently sent 23 boxes containing protected health information to a recycling center.** These boxes contained the names, addresses, Social Security numbers, insurance identification numbers, clinical information, and credit/debit card numbers of 1,590 individuals. Following the breach, the covered entity reviewed its policies and procedures, suspended several employees, and set up credit monitoring for those individuals affected. As a result of OCR's investigation, the covered entity placed a record into its accounting of disclosure log for each member impacted, terminated the suspended employees, revised its policies and procedures, and retrained staff.



# Examples of HIPAA Violations

On April 6, 2010, the covered entity learned that a filing cabinet it donated to a non-profit organization on December 20, 2009, contained members' protected health information (PHI). The cabinet contained the PHI of approximately 12,000 individuals. The PHI involved member information for Medicare Health Surveys from 2001 to 2004, which contained names, addresses, telephone numbers, Social Security numbers, and Medicare identification numbers. Following the breach, the covered entity notified the affected individuals of the breach, notified the media, sanctioned the employees involved in the incident, held a mandatory training for all departments involved in the breach regarding Privacy, Security, and Compliance rules, regulations, and responsibilities, revised the policy for office moves requiring a series of checklists and approvals prior to moving furniture offsite, and offered all affected individuals free credit monitoring, including assistance with identify theft protection.

An unencrypted laptop computer was stolen from the covered entity's unlocked testing office. The laptop computer contained the protected health information of approximately 689 individuals. The protected health information involved in the breach included names, dates of birth, Social Security numbers, and the age, gender, race, and medication information of affected individuals. Following the breach, the covered entity restricted the storage of electronic protected health information to network drives. Additionally, OCR's investigation resulted in the covered entity improving their physical safeguards and in retraining employees.