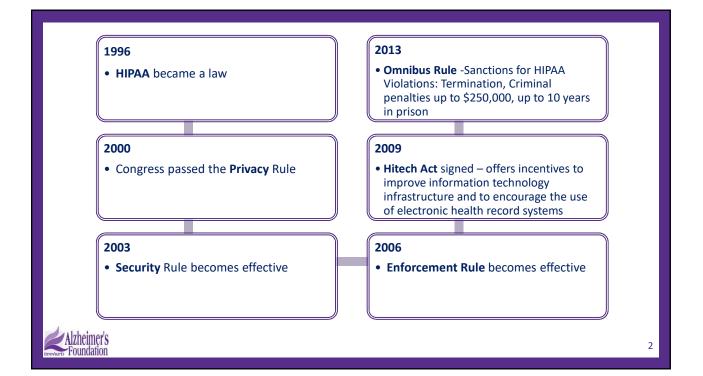




HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

www.training.brevardALZ.org



4

# PRIVACY AND CONFIDENTIALTY

All businesses have a legal and ethical responsibility to safeguard the **privacy** of all patients and **protect the confidentiality of their health information.** 



### WHAT IS HIPAA?

- <u>H</u>ealth Insurance Portability and Accountability Act
- Creates national standards for privacy and security of patient information
- Defines certain patient rights such as the patient's right to access his/her medical record information



### **PARTS OF HIPAA**

#### 1. Privacy

Protects the privacy of clients

#### 2. Security

 Controls the confidentiality of electronically protected health information (ePHI), including how it is stored and accessed

#### 3. Electronic Data Exchange

 Defines the format of electronic transfers of information between providers and payers to carry out financial or administrative activities related to healthcare including coding, billing, and insurance verification



### WHAT INFORMATION IS PROTECTED?

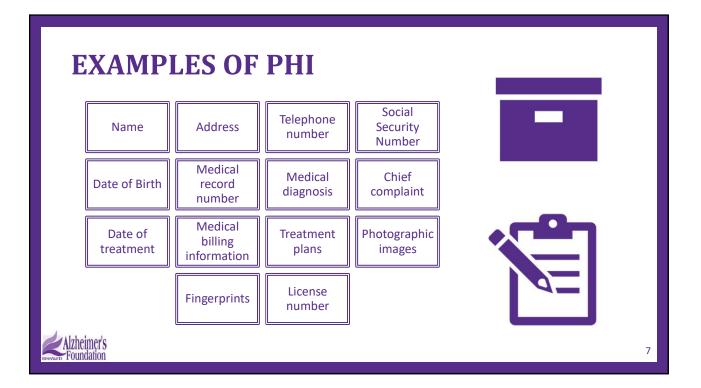
#### 1. Protected Health Information (PHI)

- Any information that can identify the individual
- Information about patients and their past, present, or future health conditions
- All information about patient maintained in electronic paper, oral, or paper format

#### 2. Electronic Protected Health Information (EPHI)

Information about patients that is kept in electronic form on computers





# WHO MUST COMPLY WITH HIPAA RULES?

- 1. **Covered Health Care Providers** every healthcare provider who electronically submits health information (doctors, clinics, etc.)
- 2. Health Plans entities that provide or pay the cost of medical care (Insurance, HMOs, etc.)
- 3. Health Care Clearinghouse entities that processes healthcare transactions (billing services, repricing companies, etc.)
- 4. Business Associates a person or organization using/disclosing individually identifiable health information to perform/provide services for a covered entity (financial/legal services, accreditation, etc.)

#### MINIMUM NECESSARY STANDARDS OR "NEED TO KNOW RULES"

- Limits PHI to minimum necessary in ALL forms (electronic, written, oral)
- Limits uses, disclosures, and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request
- Entire health record should not be used unless it is required for the intended purpose and/or treatment of the client
- Example: if you are billing Medicare for a client's health assessment, you do <u>not</u> need the client's full medical record or assessment results. You <u>only</u> need enough information to process the payment.



### **AUTHORIZATION**

- Written authorization is required to disclose any PHI
- A copy of the completed/signed authorization must be given to the client
- NOTE: a client may revoke an authorization at any time
- Authorization does not mean release <u>ALL</u> information



10

### **PERMITTED USES AND DISCLOSURES**

The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for:

- Treatment, Payment, and Healthcare Operations (TPO)
- Required disclosure to the client or to Health & Human Services (HHS) Department for compliance
- As required by law
- Law enforcement purposes
- To prevent serious threat to health and safety
- To report victims of abuse, neglect, domestic violence or injury
- Judicial proceedings
- Workers' compensation

Alzheimer's Foundation

#### **GOOD PRACTICES TO PROTECT PHI**

Talk quietly

client names
Use only first name and last initial if needed

Avoid using

Discuss in private (behind closed doors) Avoid public areas (hallways, breakrooms, etc.)

#### YOU NEVER KNOW WHO MAY OVERHEAR YOUR CONVERSATION

Do not leave PHI:

- With anyone who is not authorized to receive it
- Unattended in a door, hallway, or mailbox

# TRANSPORTING PHI

- Make sure you have supervisor permission first
- Carry in a locked, closed, or sealed container
- Names should not be visible
- Store in the trunk of your vehicle or out of sight in vehicle





### **HIPAA SECURITY RULE**

- How we protect our computer systems and how we control access to our client's electronic PHI
- Use unique usernames and complex passwords to access PHI
- Always "log off" or lock computer when not in use
- Keep building secure
- Wear ID badges at all times
- Require visitors to wear ID badges



#### • One sheet of paper containing PHI left at the front desk visible to others (sign-in sheet) - PRIVACY Computer left unattended while logged in – SECURITY • Knowingly releasing medical record or other PHI to **EXAMPLES OF** unauthorized individuals - PRIVACY NON-• Example: a caregiver asks for another patient's **COMPLIANCE &** name/contract info/medical diagnosis **UNAUTHORIZED** Verifying to unauthorized entity the enrollment, diagnosis, or treatment of another individual -**DISCLOSURES** VARIABLE Example: telling a random volunteer that a patient does attend the day care and has since 2016. **Alzheimer's** 16

#### • Medical records area left unattended, and door open to a public hall – **PRIVACY** • Example: leaving the nurses' door open with charts sitting on the desk with no one in the office **EXAMPLES OF** • Sharing your computer login with another staff member - SECURITY NON-• Driving with unsecured medical records or other **COMPLIANCE &** patient's PHI in vehicle - PRIVACY **UNAUTHORIZED** • Leaving medical records on one's desk in an unlocked **DISCLOSURES** office in an area with public access - PRIVACY • Faxing of PHI to an unsecured office fax machine -SECURITY Alzheimer's 17

# **CLIENT RIGHTS**

**01** Right to receive the Notice of Privacy Practices

02 Right to copy of PHI (electronic or paper)

03 Right to ask for corrections to PHI

04 Right to request Confidential Communications

05 Right to request a Restriction on who can access their PHI

06 Right to receive a Breach Notification

07 Right to an Accounting of Disclosures



**AND FINALLY...** WE HAVE A LEGAL, MORAL, AND ETHICAL RESPONSIBILITY TO **PROTECT PATIENT INFORMATION** AS IF IT WERE OUR OWN.

**HIPAA IS EVERYONE'S RESPONSIBILITY, AND EVERYONE IS RESPONSIBLE FOR REPORTING HIPAA VIOLATIONS.** 



#### Name: \_\_\_\_\_ Date: \_\_\_\_\_ **POST-TEST** HIPAA stands for Health Insurance \_\_\_\_\_\_ and Accountability Act. 1. 2. Protecting P\_\_\_\_\_\_ is the utmost concern of HIPAA. 3. PHI stands for \_\_\_\_\_ 4. Authorized Disclosures are allowed under HIPAA. **TRUE OR FALSE** It is not necessary for an employee to consult their supervisor before disclosing PHI. TRUE OR FALSE 5. A valid authorization may contain a statement of an individual's right to revoke the authorization in writing. 6. **TRUE OR FALSE** 7. We should avoid any discussion regarding health issues using client names in public areas. TRUE OR FALSE Clients may not review their health records without written permission from their doctor. TRUE OR FALSE 8. Leaving client medical records open in the hallway is not a HIPAA violation if only for a few minutes. TRUE OR 9 FALSE 10. A caregiver asks if long time neighbor is also attending Joe's Club. Under HIPAA you can verify this information. TRUE OR FALSE **Alzheimer's** 20 Foundation