Alzheimer's Foundation Brevard

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

www.training.brevardALZ.org

1996
- **HIPAA** became a law

2000
- Congress passed the **Privacy** Rule

2003
- **Security** Rule becomes effective

2006
- **Enforcement Rule** becomes effective

2009
- **Hitech Act** signed – offers incentives to improve information technology infrastructure and to encourage the use of electronic health record systems

2013
- **Omnibus Rule** -Sanctions for HIPAA Violations: Termination, Criminal penalties up to $250,000, up to 10 years in prison

Alzheimer's Foundation Brevard

2

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.**

Alzheimer's Foundation Brevard

3

WHAT IS HIPAA?

- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
- 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

Alzheimer's Foundation Brevard

4

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

Alzheimer's Foundation Brevard

5

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

Alzheimer's Foundation Brevard

6

EXAMPLES OF PHI

Name	Address	Telephone number	Social Security Number
Date of Birth	Medical record number	Medical diagnosis	Chief complaint
Date of treatment	Medical billing information	Treatment plans	Photographic images
	Fingerprints	License number	

Alzheimer's Foundation of Brevard

7

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.)

Alzheimer's Foundation of Brevard

8

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 not need the client's full medical record or assessment results. You only need enough information to process the payment.

Alzheimer's Foundation Brevard

9

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 **ALL** information

Alzheimer's Foundation Brevard

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 Brevard

11

GOOD PRACTICES TO PROTECT PHI

Talk quietly	Avoid using client names • Use only first name and last initial if needed	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

Alzheimer's Foundation Brevard

12

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

Alzheimer's Foundation Brevard

13

SECURING PHI IN THE OFFICE

Lock up PHI in drawer/cabinet or shut the door when leaving the office

Keep PHI out of view so others cannot easily see it by turning it over or covering it

Do not leave PHI unattended in copy / fax machines

Shred confidential papers or place in designated, secure, confidential paper bin

Alzheimer's Foundation Brevard

14

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

Alzheimer's Foundation Brevard

15

EXAMPLES OF NON-COMPLIANCE & UNAUTHORIZED DISCLOSURES

- 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 unauthorized individuals – **PRIVACY**
  - Example: a caregiver asks for another patient's name/contract info/medical diagnosis
- Verifying to unauthorized entity the enrollment, diagnosis, or treatment of another individual – **VARIABLE**
  - Example: telling a random volunteer that a patient does attend the day care and has since 2016.

Alzheimer's Foundation Brevard

16

EXAMPLES OF NON-COMPLIANCE & UNAUTHORIZED DISCLOSURES

- 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
- Sharing your computer login with another staff member - **SECURITY**
- Driving with unsecured medical records or other patient's PHI in vehicle – **PRIVACY**
- Leaving medical records on one's desk in an unlocked office in an area with public access – **PRIVACY**
- Faxing of PHI to an unsecured office fax machine – **SECURITY**

Alzheimer's Foundation Brevard

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

Alzheimer's Foundation Brevard

18

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.

Alzheimer's Foundation Brevard

19

Name: _____ Date:_____

POST-TEST

1. HIPAA stands for Health Insurance _____ and Accountability Act.
2. Protecting **P**_____ is the utmost concern of HIPAA.
3. PHI stands for _____.
4. Authorized Disclosures are allowed under HIPAA. **TRUE OR FALSE**
5. It is not necessary for an employee to consult their supervisor before disclosing PHI. **TRUE OR FALSE**
6. A valid authorization may contain a statement of an individual's right to revoke the authorization in writing. **TRUE OR FALSE**
7. We should avoid any discussion regarding health issues using client names in public areas. **TRUE OR FALSE**
8. Clients may not review their health records without written permission from their doctor. **TRUE OR FALSE**
9. Leaving client medical records open in the hallway is not a HIPAA violation if only for a few minutes. **TRUE OR 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 Foundation Brevard

20