CENTRAL STATE COMMUNITY SERVICES ANNUAL CORPORATE COMPLIANCE TRAINING

HIPAA

HIPAA TRAINING OBJECTIVES

- By the end of this training participants should be able to:
- Discuss the background and purpose of the Health Insurance Portability and Accountability (HIPAA) privacy rule.
- Identify ways in which HIPAA applies to employees of Central State
- Review basic HIPAA definitions
- Apply HIPAA basics in a workplace setting

WHAT IS HIPAA

- HIPAA is a federal law enacted in 1996.
- The original intent of HIPAA was to reduce costs, simplify administrative processes, and improve the privacy and security of individuals' health information in the healthcare industry.
- HIPAA's Privacy Rule was enacted to protect the confidentiality of patients' health information.

DEFINITIONS

- Covered Entity (CE)- Healthcare providers, health plans, and healthcare clearinghouses who electronically transmit any health information
- Protected Health Information (PHI)- Information the CE creates or receives that identifies the patient, including demographic information (e.g., addresses, phone numbers, etc.). PHI can relate to the past, present, or future physical or mental health or condition of a patient.
- Business Associate (BA)- A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE.
- Breach- A forbidden use or disclosure of PHI that compromises the security or privacy of PHI.

TO WHOM DOES HIPAA APPLY?

- HIPAA applies to all staff (including temporary staff, contract workers, and volunteers) and any vendors (business associates) that have access to PHI.

EMPLOYEES OF CENTRAL STATE

- As an employee of Central State Community Services, you have a duty to:
  - Maintain confidentiality of all resident's PHI as required by law.
  - Use, view, or discuss patients' PHI only as required by job responsibilities
  - Understand HIPAA policies
  - Immediately notify the organization's privacy officer of any suspected or actual breach of patients' PHI
  - Direct questions or concerns to the organization's privacy officer

CENTRAL STATE'S PRIVACY POLICY

- Central State Community Services has a privacy policy to ensure that electronic and paper documents are secure.
- Electronic: Computers are installed with screen savers to block the view of information when the computers are not in use. Each username and password to protect the access of the information
- Paper: At the administrative office, each office has a mailbox next to each door. Paper documents are to be placed in the box to face the wall, so privacy is protected.
- Paper documents are placed in a sealed envelope to protect privacy in the homes.
- Confidential mail is opened and filed
- Paper in file bins or sorting bins are placed face down.

RELEASING A RESIDENT'S PHI

- Residents and guardians have a right to:
- View and receive a copy of their medical records
- Request amendments or changes to their medical records
- Request restrictions to the use or disclosure of their PHI
- Request an accounting of the disclosures of their PHI

RELEASING PHI BASIC RULES

- Patients' information can be released without authorization if the purpose is for treatment, payment, or healthcare operations.
- Disclosure of patients' PHI for anything other than treatment, payment, or healthcare operations requires completion of an authorization.
- Certain exceptions exist for public health monitoring activities (e.g., disease reporting), government oversight, and some law enforcement investigations

Staff should always consult with the privacy officer to ensure proper release.

DISCLOSURE OF PHI TO BAs

- Authorizations are not required for a business associate who perform certain functions for the Covered Entity.
- Examples of BAs include billing companies, transcription services, IT vendors, and accountants.
- Patient authorizations are not necessary for BAs; however, business associate agreements set out the duties required of the BA to protect patients' PHI are required.

WHAT IS THE MINIMUM NECESSARY STANDARD?

- Whenever resident's PHI is used or disclosed, whether to another CE or BA, only the information necessary to accomplish the intended purpose should be disclosed.

- Example: CMH is requesting information regarding a particular resident. Employees do not give out information about other residents or their families.

BREACH NOTIFICATION EXAMPLES

- Looking at a neighbor's medical record out of curiosity
- Losing an unencrypted thumb drive
- Talking to a family member about a resident without proper consent
- Providing records to an attorney without authorization
- Lost or stolen computer that contains PHI

Staff should immediately notify a Supervisor or Program Coordinator if they suspect or discover a breach has occurred.

CIVIL AND CRIMINAL PENALTIES

- Failure to comply with policies and procedures may result in corrective action.
- CEs (including individual employees) and BAs are subject to civil monetary penalties (fines) and criminal penalties.
- Knowingly obtaining or disclosing PHI without authorization - Up to $50,000 fine and 1 year in prison
- If done under false pretenses - Up to $100,000 fine and 5 years in prison
- If done with intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm -Up to $250,000 fine and 10 years in prison

SUMMARY

- Be familiar with HIPAA policies in your organization and how they specifically affect your job role.
- Understand patients' rights in relation to reviewing, requesting, and releasing PHI.
- Understand rules in relation to the release of PHI to BAs, as well as the concept of "minimum necessary standard."
- Promptly report any suspected breaches
- Don't hesitate to ask questions

TEST