easterseals
Northern California

HIPAA 101

Compliance is Everyone's Job

February 24, 2022

What is HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is federal law passed in 1996 which addresses issues ranging from health insurance coverage to national standard identifiers for healthcare providers.

The portions that are important for our purposes are those that deal with protecting the privacy (confidentiality) and security (safeguarding) of health data, which HIPAA calls Protected Health Information or PHI.

easterseals Northern California

What is Protected Health Information? (PHI)

- Any information, transmitted or maintained in any medium, *including demographic information.*
- Created/received by covered entity or business associate.
- Relates to/describes past, present or future physical or mental health or condition; or past, present or future payment for provision of healthcare; and
- Can be used to identify the client.

easterseals Northern California

Types of Data Protected by HIPAA

- Written documentation and all paper records.
- Spoken and verbal information including voice mail messages.
- Electronic databases and any electronic information, including research information, containing PHI stored on a computer, smart phone, memory card, USB drive, or other electronic device.
- Photographic images.
- Audio and Video recordings.

easterseals Northern California

To De-Identify Client Information You Must Remove All 18 Identifiers

- Names
- Geographic subdivisions smaller than state (address, city, county, zip)
- All elements of DATES (except year) including DOB, admission, discharge, death, ages over 89, dates indicative of age
- Telephone, fax, SSN#s, VIN, license plate #s
- Med record #, account #, health plan beneficiary #
- Certificate/license #s
- Email address, IP address, URLs
- Biometric identifiers, including finger & voice prints
- Device identifiers and serial numbers
- Full face photographic and comparable images
- *Any other unique identifying #, characteristic, or code*

easterseals Northern California

Department of Justice-Imposed Criminal Penalties for Employee

- Wrongfully Accessing or Disclosing PHI: Fines up to $50,000 and up to 1 Year in Prison.
- Obtaining PHI Under False Pretenses: Fines up to $100,000 and up to 5 Years in Prison.
- Wrongfully Using PHI for a Commercial Activity: Fines up to $250,000 and up to 10 Years in Prison.
- HIPAA criminal and civil fines and penalties can be enforced against INDIVIDUALS as well as covered entities and Business Associates who obtain or disclose PHI without authorization.

easterseals Northern California

HIPAA Sanctions

Employees, interns, and volunteers who do not follow HIPAA rules are subject to disciplinary action.

Sanctions depend on severity of violation, intent, pattern/practice of improper activity, etc., and might include:

- Dismissal from participating in the internship program.
- "Mandatory sanctions for breach of confidentiality or of other client related duties, with the sanction severity increasing for careless or willful breach of such duties." FoC Employee Handbook page 32.

Civil and/or criminal penalties including incarceration.

easterseals Northern California

Working from home presents privacy & security risks

Consider these tips:

- Avoid connecting to public Wi-Fi
- Keep work only on your work computer
- Do not leave materials containing PHI viewable on desks or counters
- Encrypt sensitive data when sharing via email or in the cloud
- Keep up with privacy & security training

easterseals Northern California

Breach Notification

HIPAA requires that we notify affected individuals and federal officials when a breach or potential breach of privacy has occurred.

. The following slides discuss:

- The types of breaches requiring client notification and those that are exempt.
- Time in which the notification must occur.
- Responsibility of employee to report any incident.

easterseals Northern California

What is a Breach?

- Breach is defined as the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the information.

- Impermissible use or disclosure is presumed to be a breach unless the facility or business associate proves that there is a low probability that PHI has been compromised.

easterseals Northern California

Exceptions When Breach Notification Not Required

Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if made in good faith or within course and scope of employment.

Inadvertent disclosure of PHI from one person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.

Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

easterseals Northern California

Security Standards – General Rules

HIPAA security standards ensure the confidentiality, integrity, and availability of PHI created, received, maintained, or transmitted electronically (PHI –Protected Health Information) by and with all facilities.

Protect against any reasonably anticipated threats or hazards to the security or integrity or such information.

Protect against any reasonably anticipated uses or disclosures of such information that are not permitted.

easterseals Northern California

Rules for Protecting Information

- Do not allow unauthorized persons into areas where access to PHI could occur.
- Arrange computer screens so they are not visible to unauthorized persons and/or clients; use security screens in areas accessible to public.
- Log in with password, log off prior to leaving work area, and do not leave computer unattended.
- Lock up files or paperwork containing PHI that is not in use .
- Do not duplicate, transmit, or store PHI without appropriate authorization.
- Storage of PHI on unencrypted removable devices (Disk/CD/DVD/Thumb Drives) is prohibited without prior authorization.

easterseals Northern California

Glossary of Terms

Administrative Safeguards
Administrative actions and policies and procedures (1) to manage the selection, development, implementation, and maintenance of security measures, and (2) to protect ePHI and to manage the conduct of the Covered Components' workforce in relation to the protection of ePHI.

Business Associate (BA)
A person or organization hat performs a function or activity on behalf of a covered entity but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

Covered Entity (CE)
Any business entity that must comply with HIPAA regulations, which includes health-care providers, health plans and health-care clearinghouses. For purposes of HIPAA, health-care providers include hospitals, physicians and other caregivers.

easterseals Northern California

Glossary of Terms continued

Covered Entity continued
Catalight Foundation is the covered entity for HIPAA compliance purposes.

DHHS
US Department of Health and Human Services.

Disclosure
The release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.

HIPAA
Health Insurance Portability and Accountability Act of 1996.

easterseals
Northern California

Glossary of Terms continued

Individual – the person who is the subject of PHI.

Individually Identifiable Health Information (also called PII)
A subset of "health information," including demographic information, (1) that is created or received by a health care provider, health plan, employer, or health care clearinghouse; 2) that relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and (3) that identifies the individual or might reasonably be used to identify the individual.

OCR
Office of Civil Rights, the branch of the DHHS that is responsible for federal oversight of the privacy regulations.

easterseals Northern California

Glossary of Terms continued

Privacy Rule
The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.

Protected Heath Information (PHI or ePHI)
Is any individually identifiable health information, including genetic information and demographic information, collected from an individual, whether oral or recorded in any form or medium that is created or received by a covered entity.

easterseals Northern California

Glossary of Terms continued

Protected Heath Information (PHI) continued

PHI encompasses information that identifies an individual or might reasonably be used to identify an individual and relates to:

- The individual's past, present or future physical or mental health or condition of an individual; OR
- The provision of health care to the individual; OR
- The past, present or future payment of health care to an individual.

Information is deemed to identify an individual if it includes either the client's name or any other information that taken together or used with other information could enable someone to determine an individual's identity. (For example: date of birth, medical records number, health plan beneficiary numbers, address, zip code, phone number, email address, fax number, IP address, license numbers, full face photographic images or Social Security.

Glossary of Terms continued

Technical safeguards

Are the technology, and the policy and procedures for its use that protect electronic protected health information and control access to it.

easterseals Northern California