HIPAA TRAINING

2019

Privacy Officer and Security Officer

- Privacy Officer – Designated employee responsible for development and implementation of privacy policies and procedures, training, monitoring and management of PHI breach incidents.
  - Kevin Harding, Director of Information Technology

- Security Officer – Designated employee responsible for coordinating compliance with HIPAA Security Rule to ensure physical and electronic security of properties and information systems.
  - Kevin Harding, Director of Information Technology

Disclaimer

HIPAA regulation is expansive and complex.

1. Within most sections, there are exceptions.
2. "Can I…" questions are routine and expected.
   - Frequently utilize outside resources to troubleshoot.
3. Assessment of PHI breaches involves interpretation of rule. Legal sanctions tend to guide assessments and interpretations.
4. Ongoing learning!

Who Does HIPAA Apply To?

- Covered Entities
  - Health Plans
  - Health Care Clearinghouses (entities that facilitate electronic transactions by "translating" data between health plans and providers when they use non-compatible information systems)
  - Health Care Providers who transmit health information in electronic form in connection with one or more of the list of covered transactions

- Business Associates of a covered entity

Imagine! is both a Covered Entity AND a Business Associate. As an employee of Imagine!, HIPAA applies to YOU.

Privacy Rule

Body of federal regulation within the Administrative Simplification section that provides comprehensive protection of individual's health information.

- Guidelines on:
  1. Use and disclosure of PHI
  2. Required notice of privacy practices
  3. An individual's rights concerning his/her PHI
  4. Administrative requirements that CEs must take

Privacy Rule

Purpose of Privacy Rule:

1. Gives consumers/guardians more control over their health information.
2. Sets boundaries on use and disclosure of PHI.
3. Establishes appropriate safeguards CEs and others must take to protect consumer information privacy.
4. Holds CEs accountable with civil and criminal penalties if rules are violated.

The Privacy Rule impacts “protected health information”.

Protected Health Information (PHI)

- Any health information maintained by Imagine! that is individually identifiable except (a) employment records and (b) information regarding a person who has been deceased for more than 50 years.
- Any health information, including demographic information, in any form or medium, that:
  - Is created or received by a healthcare provider, or healthcare clearing house; and,
  - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and,
    - That identifies the individual; or,
    - There is a reasonable basis to believe the information can be used to identify the individual.

All information about the individuals we serve, including name, services, diagnosis information, etc., is considered PHI. All health information maintained by Imagine! is individually identifiable unless de-identified.

Common PHI Identifiers

1. Names
2. Social security numbers
3. Addresses
4. Birth dates
5. Photos
6. Insurance numbers
7. Biometric identifiers, including fingerprints and voice recordings
8. Information about someone with a rare disease*

Minimum Necessary Standard

- The least amount of PHI needed to achieve the intended purpose of the use or disclosure.
- Imagine! is required to limit the amount of PHI it uses, discloses, or requests to the minimum necessary to do the job.

Treatment, Payment, and Operations (TPO)

HIPAA allows the sharing of information for purposes of TPO.

- Treatment:
  - The use of information for the purpose of providing continuing services.
- Payment:
  - Sharing information in order to bill for the provision of services to the person served.
- Operations:
  - Certain administrative, financial, legal, and quality improvement activities that are necessary for Imagine! to run its business and support the core functions of treatment and payment.

An Authorization to Release Information is <u>not</u> required in circumstances that fall under TPO.

Authorization to Release Information

- A signed statement of agreement to the use or disclosure of Protected Health Information (PHI).

- When PHI is to be used or disclosed for purposes other than the continuing care of persons in services (treatment), payment of services, or the coordination of care and day to day operations of Imagine! (operations), Imagine! should disclose such information as outlined on a valid, written authorization received from the person in services, their parent (if a minor), or legal guardian.

Exceptions to Authorization Requirements

PHI may be disclosed by the Privacy Officer or his/her designee without an authorization if the disclosure is:

1. For TPO;
2. As required by State or Federal law*;
3. An administrative request, subpoena, or investigative demand*;
4. Disclosure will prevent or lessen a serious or imminent threat to the health or safety of a person or the public*;
5. To law enforcement authorities to identify or apprehend an individual*.

Disclosures should be forwarded/reported to the Privacy Officer or Security Officer.

Situations that Require an Authorization to Release Information

- Family members
- ACL
- Law Enforcement (Detective, Probation/Parole Officer, Police Officer); HIPAA generally prohibits the disclosure of PHI to law enforcement unless the individual has provided written consent or other conditions are met
- Media/PR
- Law firms
- Schools
- DVR

Situations that (GENERALLY) do NOT Require an Authorization to Release Information

- Doctor's offices to obtain PMIPs
- Guardians
- PASAs
- Host Homes
- Other CCBs
- ACMI
- Contractors of Imagine!
- Mental Health Partners

The Bottom Line

- When in doubt, obtain an Authorization!
- The lists are guidelines – information sharing must be for TPO purposes.
- HIPAA law is complex. Many organizations choose to request/forward an Authorization to Release Information even if TPO applies.

Incidental Use and Disclosure

- Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the CE has applied reasonable safeguards and implemented the minimum necessary standard.

- A secondary use or disclosure that cannot be reasonably prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule.

- CEs must have appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by Privacy Rule.

- It is not expected that safeguards guarantee privacy of PHI from any and all potential risks. Reasonable safeguards vary from CE to CE depending on factors such as size of agency and nature of its business. CE must take into consideration the potential effects on consumer care and may consider other issues, such as financial and administrative burdens, of implementing particular safeguards.

Employees of Imagine! shall not discuss identifying information about an individual seeking or receiving services/supports in public, in public areas of Imagine! offices, nor with individuals not entitled to protected health information.

Examples of Safeguards

- Speaking quietly in public areas about a consumer's services.
- Avoiding the use of full names of consumers in public areas including hallways and restaurants.
- Locking file cabinets and records rooms.
- Turning documents with PHI upside down on fax machine, printer, or your desk.
- Password protecting electronic devices such as smart phones and computers.
- Using the minimally necessary amount of PHI

Management of Records Containing PHI

- Records (permanent files and working files) containing PHI should be kept in a place inaccessible to the general public (locked cabinets or locked room).

- Staff members who remove hard consumer folders from a records cabinet or room should sign the file in/out. While the file is checked out, the employee will store the file in a locked drawer when away from their work station.

- When travelling between locations with working files, files containing PHI should be carried in the locked trunk of the vehicle in which they travel. If the vehicle does not have a trunk the files should be carried in a locked container such as a briefcase. If this is not feasible, the files should be carried in a closed container such as an envelope, file folder or notebook which does not identify the contents of the container, and placed in the vehicle in such a way that the opportunity for public viewing is minimized.

- If traveling staff must occasionally keep files in their homes they must be stored in such a manner that they are not accessible to other members of the household.

Daily Routines to Safeguard PHI

- All computers must have screen savers that activate after a period of inactivity. The screen saver may only be deactivated by an employee's password.
- Only encrypted USB drives will be used to transport PHI (available through IT).
- All trash that contains PHI must be placed in the designated receptacles to be shredded. The receptacles must be locked or located in offices/rooms that can be locked when the Imagine! offices are closed.
- Fax machines and collectively used printers will be located in areas that are not accessible to the general public. When faxes are received, or documents are printed, designated staff will periodically remove documents from the respective machines, if they have not been claimed by the person for whom the document is intended, and place them in the mail folders or mailboxes designated for each staff person.
- When PHI is being provided to Imagine! staff in designated mailboxes, the information should be contained in envelopes or other containers that protect the confidentiality of that information.

Electronic Communication and Mobile Devices

- Emails containing PHI should be sent encrypted (NeoCertified)

  Workarounds:

  1. Remove identifying PHI
  2. Start a new email thread without PHI
  3. Concerned about NeoCertified going to junk mail? Send a separate email alerting end user of incoming encrypted email.

- PHI should never be transmitted via text message.

- After emailing a photo (scan) of a document containing PHI via secure email, completely delete the image from your mobile device.

PHI Breaches

- It is expected that staff will report all violations to the Privacy Officer or, in her absence, the Security Officer.
- Reports should be made ASAP.
- Refer to the Employee Handbook for sanctions against the employee for delayed reporting or lack of reporting.

Notice of Privacy Practices

- All individuals applying for Imagine! services should receive this during their Intake process
- This document describes:
  - The type of information collected and maintained;
  - Who collects the information and how;
  - Storage and maintenance of the information;
  - The anticipated use and routine disclosure of the information.

Access to PHI

- An individual has the right to inspect and obtain a copy of PHI by:
  1. Viewing the information in the record.
  2. Electronic duplication of the information in the record.
  3. Responding to telephone inquiries about the consumer and/or about information in the record.
  4. Participating in meetings where identifying information is discussed.

- Individuals do not have the right to access:
  1. Psychotherapy notes
  2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Requests for copies of the consumer file must be submitted, in writing, to the Privacy Officer. Requests will be reviewed and responded to within 30 days.

Requests for amendments to the consumer file must be submitted, in writing, to the Privacy Officer. Requests will be reviewed and responded to within 30 days.

Q/A

Can I send an email unencrypted if the guardian asks me to?

No

- Email containing PHI that will leave our servers must be encrypted (hint: if the email address is not xyz@imaginecolorado.org, it is leaving our network.)
- HIPAA outlines Encryption as a Standard; it provides protections to Imagine!. Organizations can choose to use it or not – Imagine! uses it.
- Future HIPAA Procedures will create a process for an individual to waive the protections of encryption.

Do I need to use NeoCertified for all of my emails containing PHI?

If they leave our network, yes.

- If there is a reasonable basis to believe the information could identify a person, it is PHI.
- When responding to email chains containing PHI, you can start a new chain or remove the PHI to avoid using NC.
- Keep email chains tight.

Do I need an Authorization to share information with a prospective provider, including Imagine! FREs?

As long as minimum necessary information is shared and it is for the purpose of a potential referral for services to another HIPAA covered provider, no.

- PHI exchanged should be in a secure manner (encrypted email, etc.).
- In the IDD world, providers are PASAs of the state and contractors of Imagine!.
- If you are unsure if someone is considered a provider under HIPAA, use an Authorization or ask.

Do I need an Authorization to consult with my client's doctor?

No.

- This type of PHI falls under "Treatment, Payment, and Operations" because the sharing of information allows you and the physician to coordinate care.

If I get a call from a police officer accompanying my client in the hospital, requesting their address to get them home, can I share it?

Yes.

- Information shared should be limited to the minimum necessary amount of information to safely transport the individual home.

If someone shows up with a subpoena, do I need to immediately turn over my client's information?

No.

- All subpoenas must be forwarded to the Privacy Officer for review prior to disclosing any PHI. There are different types of subpoenas, some which require the consent of the individual prior to releasing their PHI.

If my client has a guardian, and also parents who are still involved, can I share PHI with those parents without an Authorization?

No.

- Guardians must sign an Authorization permitting Imagine! to share information with parents who are not guardians. Colorado law gives guardians the authority to make decisions regarding their ward's support, care, health, and welfare including consenting to an Authorization to Release Information.
- If you face resistance from the parents, forward them to the Privacy Officer for additional communication.

If I am concerned that my client doesn't understand what he is signing, but he is a free agent, can he sign?

Yes.

- All adults are considered legally capable of making decisions regarding their personal and financial affairs *unless and until* a court of law determines otherwise.

Can I share information with a hospital without an Authorization?

Yes.

- PHI disclosure is permissible under TPO for shared clients.

Can my client share their own information with whomever they like?

Yes.

- PHI belongs to the individual we are serving. They can share their information freely.
- If you run into Authorization issues, remember the client or guardian can share whatever information they want.