HIPAA Privacy & Security Training 2024

Introduction

HIPAA training for healthcare workers is a requirement of both the Privacy Rules and the Security Rule. In addition, Covered Entities may need to provide further HIPAA training for healthcare workers if a threat to the confidentiality, integrity, or availability of ePHI that could be mitigated by further training is identified in a risk assessment.

- Integrated Home Care Services (IHCS) or (“Integrated”) is committed to a culture of ethical business practices and compliance.
- Integrated’s success as an industry leader is based on realizing our mission through policies and procedures.
- The purpose of this training is to provide an overview of the Health Insurance Portability and Accountability Act (HIPAA) to our Network Providers.
- Additional training may be available to address specific HIPAA requirements for your SBU or area of responsibility.

HIPAA

What is Your Role

- HIPAA permits providers, insurance companies, and other healthcare entities and business associates to exchange information necessary for treatment, payment, and healthcare business operations.
- Based on inappropriate actions or breaches in confidentiality by employees, your company or employees can be held liable and may be subject to sanctions for violations.
- IHCS employees having access to Personal Health Information (PHI) will need to ensure compliance with internal policies and federal regulations to ensure all confidential information is treated with the highest level of integrity and respect for the confidentiality of the information.
- The Company is committed to holding all operational policies and employee actions in accordance with HIPAA regulations.

Training Objectives

This Privacy Information Security Training is part of an evaluation of policies, procedures, and standards with respect to Business Associate Agreements. Elements that will be reviewed in this training focus on key risk areas that may heighten Integrated's exposure to security incidents or breaches. How employees manage regulatory oversight and what control mechanisms are in place to prevent, detect, and correct non-compliance will be validated.

- **Define the provisions of HIPAA.**
- **Recognize and understand the importance of complying with HIPAA.**
- **Understand and be able to identify examples of PHI.**
- **Understand consequences for not complying with HIPPA.**
- **Identify employee/contractors responsibility for reporting privacy and security incidents.**

What is HIPAA

The Health Insurance Portability and Accountability Act, known as HIPAA:

- Permits the disclosure of health information needed for patient care and other important purposes.
- Provides federal protection for individually identifiable health information held by covered entities and their business associates.
- Gives patients rights with respect to how their information is handled.

The requirements of HIPPA and PHI/PII protections align with Integrated's values on how we treat our customers and want you to as well!

Who Must Comply With HIPAA

Two types of organizations must comply with HIPAA:

- **Covered Entities** which include healthcare providers, like Integrated 's Home Health, DME, and Home Infusion businesses, health plans, and healthcare clearinghouses
- **Business Associates** are companies or individuals who perform services for Covered Entities and who have access to Protected Health Information received from Covered Entities
- **A Business Associate Agreement (BAA) or Data Sharing Agreement** must be signed between the provider and IHCS at the onset of business.

Protected Health Information

- **The Privacy Rules applies to a class of information known as Protected Health Information (PHI).**
- **PHI is information held or transmitted by a Covered Entity or its Business Associate that relates to:**
  - An individual's physical or mental health
  - The provision of healthcare to the individual
  - Payment for the provision of healthcare for the individual where the information gives a reasonable basis for identifying the individual

Protected Health Information - Continued

"PHI is any health-related information that can be used alone, or in combination with, other information to identify an individual."

- **Examples of PHI/PII include:**
- Name of individual
- Postal or email address
- Telephone or fax number
- Social Security number
- Date of birth
- Health, claims, and assessment related information

Protected Health Information

- Continued

- Credit card number
- Medical record
- Policy number
- Medical device identifier and serial number
- Financial account information
- Payment information

We must comply with the requirements to report and mitigate any unauthorized use or disclosure of PHI.

Minimum Necessary Standards

- **When using, disclosing, or requesting PHI, you must make reasonable efforts to limit information to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.**
- **The minimum necessary standard applies to all documented, verbal, and electronic PHI data.**
- **It is a requirement of all Integrated employees and contracted providers to uphold this commitment and requirement to the regulations.**
- **Providing quality and outstanding care for our customers is a top priority to Integrated.**

HIPAA Privacy

HIPAA…..

- Gives individuals rights to control and directly access their own health information.
- Requires all of us to protect every insured's information from unauthorized access, use, or disclosure.
- Limits uses and disclosures of PHI only to those that are authorized by the individual in writing, contractually allowed, or required by law.

Legally and Personally

Authorized Individuals

- **Personal Representatives** are authorized legally by the individual to access PHI and exercise their individual rights.
- **Authorized Individuals** are designated to have access to PHI to assist the individual, but do not have decision-making authority.
- **Certain Integrated employees** are designated with the authority to have PHI in performing the duties of their position.

Notice of Privacy Practices

The Notice of Privacy Practices:

- Contains a description of permissible uses and disclosures of PHI.
- States that an insured's written authorization is required for any use or disclosure of PHI outside of: treatment, payment, or healthcare operations.
- Explains covered entity's duties to protect health information privacy.
- Outlines HIPAA Individual Rights Requests including the right to:

- Request an amendment of incorrect PHI.
- Request an accounting of disclosures of PHI.
- Request confidential communications.
- File a complaint or an appeal.
- Request restrictions.
- Request information about privacy policies.

HIPAA Security Rule

- HIPAA regulations define the standards required for securing PHI.
- HIPAA requires organizations to ensure that all PHI, regardless of its form (e.g., paper, electronic files, email reports, spoken), are secure.
- All employees who come into contact with PHI must follow the administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI.
- Securing PHI ensures we keep our customers' trust and it also reduces the risk of incidents or HIPAA violations.
- HIPAA violations can have legal consequences and sanctions against your agency!

Technical Safeguards

- The HIPAA Security Rule requires Integrated to establish and implement administrative safeguards to manage the privacy of PHI.
- IT groups at Integrated ensure appropriate systems are in place to safeguard data internally and externally with your agency's office.
- Integrated has established its own security policies and procedures in the use, storage, disclosure, and disposition of PHI data we must comply with.

Data Security

Integrated has established data security practices including:

- Requiring passwords that consist of a combination of characters, such as upper and lowercase letters, special characters and numbers.
- Setting laptop or mobile device screensavers to require a password and appear automatically when the device is not in use.
- Prohibiting individuals from sharing passwords with anyone, including family, friends, or coworkers.
- Encrypting PHI stored on portable devices (e.g., laptops, mobile phones) and PHI that is transferred electronically (e.g., through e-mail and other online services).

Data Access and Use Instructions

Your responsibility is to:

- Follow Integrated's security policies whenever accessing, using, or disclosing PHI.
- Only access PHI if you have a legitimate need to do so.
- Limit the use and disclosure of PHI to the minimum necessary.

Security, Storage and Disposal

Facilities and Work Area

- Ensure that all IHCS facilities and work areas containing PHI are secure.
- Ensure that anyone entering a controlled area scans their badge or ID (if applicable).
- Do not allow anyone to follow you or "*piggy back*" into an area without swiping their access badge (if applicable).

Storage and Disposal

- Store PHI in secure areas.
- Dispose of documents and electronic media containing PHI in secured containers or by shredding.
- Keep mobile devices containing PHI secure.

Lost or Stolen Laptops or Company Phones

- In the event a team member's laptop is lost or stolen, the loss immediately must be reported to IHCS. An investigation needs to be conducted to determine the risk of the data and potential use of the data in violation of HIPAA regulations.

- ***Hint:*** *To avoid theft of agency equipment, all employees should demonstrate appropriate judgment in safeguarding not only the physical property of the company, but also the confidential information stored on the computer or phone.*

Work Area Instructions

Are you in Compliance with IHCS Clean Desk Top Policy?

- ✓ Keep PHI out of view from the public on desks, copiers/fax machines, whiteboards, etc.
- ✓ Make certain you quickly pull any PHI from printers and surrounding areas.
- ✓ Be aware of your surroundings when discussing or handling PHI. Do not discuss PHI in areas where unauthorized individuals can hear information being discussed.
- ✓ Discussions about any IHCS client information should be limited in a needs-to-know capacity, and specific information must not be included in any informal conversations with other employees, friends, or family members.

Enforcement and Penalties

- HIPAA has specific penalties for failing to protect PHI. Any improper release, acquisition, use, or disclosure of PHI is considered a privacy or security incident or “breach”.
- Carelessness or unintentional breaches not only violate individuals' privacy — and trust in Integrated — but also have serious consequences ranging from agency actions including warnings, suspensions or termination of contract.
- Monetary penalties from the government exist to provide consequences for those who violate HIPAA rules and regulations.
- HIPAA requires a duty to report voluntary disclosure of violations.

HITECH Act

- The HITECH Act was created to incent the healthcare industry to adopt Electronic Health Record Systems. Electronic records have a greater risk of being compromised, so increased safeguards were needed.

- The HITECH Act:
  - Strengthens the elements of the Security Rule.
  - Requires audits to ensure compliance.
  - Authorizes the State's Attorney General to bring actions under HIPAA.
  - Dramatically increases penalties for non-compliance.

Non-Compliance

For Integrated, failing to comply with HIPAA as amended by HITECH could lead to all of the following:

- Disciplinary action for our businesses and the individual
- Possible criminal penalties with up to 10 years in prison
- Personal fines up to $250,000
- Sanctions against Integrated and amplified scrutiny

Breach

- All privacy and security incidents involving PHI need to be investigated.
- All employees are responsible for reporting suspect actions immediately — no matter how minor they may appear — through our incident reporting process.
- Reporting incidents immediately can help prevent simple mistakes from turning into catastrophic breaches.
- The HIPAA Breach Risk Assessment Tool can be completed if you suspect a breach has occurred - it is an easy to use tool to measure the severity of the breach.

Complaints or inquiries from Federal or State regulators in the last two (2) years should be logged, tracked, and reported to add by IHCS. Corrective action plans on security incidents or breaches should be shared with IHCS as part of regulatory and contractual requirements. See Policy and Reporting Tool attached.*

Your Responsibilities

Retaliation against employees of Integrated Home Care Services and Network Providers who make good faith reports regarding potential violations of laws, HIPAA regulations or company policies is strictly prohibited, and violators may be subject to disciplinary action.

- Everyone who handles or maintains PHI while doing their job must comply with HIPAA.
- If you become aware of any PHI being misdirected via mail, email, fax, verbally, or otherwise, you are obligated to gather and report all relevant details to Compliance.
- By following the HIPAA Privacy and Security Rules, you support Integrated' s commitment to ensure the privacy and security of patient information.
- You also help protect Integrated's reputation and avoid costly penalties!

HIPAA Compliance

- If you have any questions regarding HIPAA compliance or your role in enforcing HIPAA rules and regulations, contact your manager, a member of the IHCS Compliance Team, or your own HR Generalist.
- Inform an IHCS Compliance Team member of any HIPAA
- disclosure or any suspected unlawful practice.
- HIPAA grants whistleblower protection from discrimination and retaliatory actions to anyone who initiates or participates in a privacy complaint process.

Compliance Contact Information

- You are obligated to report any and all HIPAA disclosures involving IHCS data to:

☎ 24 Hour Compliance Hotline 954.381.7954 or
✉ compliance@ihcscorp.com

Insurance Administration Services (IAS)

- compliance@ihcscorp.com
- Compliance Fax Line 954.624.8738
- HIPAA, Complaints, and Fraud referrals via compliance@ihcscorp.com

Integrated's Privacy Officer is Mark Gilchrist, *Ext. 7495*

HIPAA Administrative Simplification

- Continued

Trading Partner Agreements: A covered entity cannot enter into a trading partner agreement that would: (a) change the definition, data condition, or use of a data element or segment in an adopted standard or operating rule; (b) add any data elements or segments to the maximum defined data set; (c) use any code or data elements marked “not used” or that are not in a standard; or (d) change the meaning or intent of a standard. Covered entities may not agree to conduct transactions with each other that violate the adopted standards. The requirement to conduct transactions as standard transactions as described in 45 CFR§162.923(a) overrides any agreements to conduct transactions otherwise.

Summary

Integrated wants all employees to be aware of HIPAA requirements. If there are requirements that are specific to your role of SBU, additional training can be provided.

- Following is a review of the key points covered in this training:
  - HIPAA requires Integrated and her Business Associates to keep PHI private and secure for its customers.
  - PHI is health-related information that can be used alone or in combination with other information to identify an individual.
  - PHI can only be used and disclosed to the minimum necessary or need to know.
  - Unauthorized access of PHI has severe consequences to all employees.
  - Our employees are required to understand and comply with Integrated's policies and procedures as they relate to HIPAA and the handling of PHI.
  - Our employees have a responsibility and obligation to identify, and report suspected privacy and security incidents and violations.