INTEGRATED
HOME CARE SERVICES

HIPAA PRIVACY & SECURITY TRAINING

All
Employees/Contractors
2020

INTRODUCTION

- **Integrated Home Care Services 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)**
- **Additional training may be available to address specific HIPAA requirements for your SBU or area of responsibility**

INTRODUCTION

- 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/contractors, Integrated and individuals or employees can be held liable and may be subject to sanctions for violations
- Integrated employees/contractors 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
- is committed to holding all operational policies and employee actions in accordance with HIPAA regulations

TRAINING OBJECTIVES

- Define the provisions of HIPAA
- Recognize and understand the importance of complying with HIPAA
- Understand and be able to identify examples of PHI
- Identify the actions needed to secure PHI
- Understand Integrated's consequences for not complying with HIPAA
- Identify employee/contractors responsibilities for reporting privacy and security incidents

WHAT IS HIPAA?

The Health Insurance Portability & 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 HIPAA and PHI requirements align with Integrated values on how we want to treat our customers

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 clearing houses
- **Business Associates** are companies, like Integrated 's IAS division or the IHC network development team, or individuals who perform services for Covered Entities and who have access to Protected Health Information from Covered Entities

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

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

- Examples of PHI include:

- **Name of individual**
- **Postal or email address**
- **Telephone or fax number**
- **Social Security number**
- **Date of birth**
- **Health, claims and assessment related information**
- **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 STANDARD

- **When using, disclosing or requesting PHI, Integrated 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 to uphold our 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 Integrated 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 & PERSONALLY AUTHORIZED INDIVIDUALS

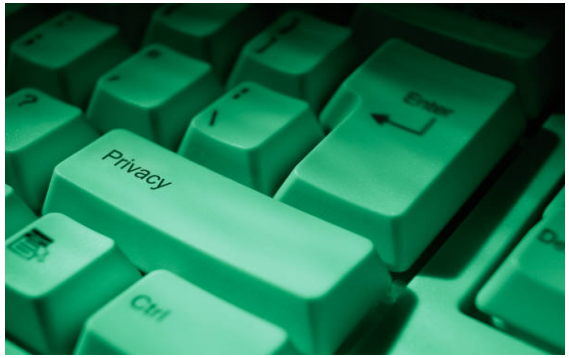
- Personal Representatives are legally authorized by the individual to access PHI and exercise their individual rights
- Authorized Individuals are designated to have access to PHI to assist the individual, but do not have decision making authority
- Certain Integrated employees are designated with the 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 health care 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/contractors 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 Integrated

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
- Integrated has established security policies and procedures in the use, storage, disclosure, and disposition of PHI data

DATA SECURITY AT INTEGRATED

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 & 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 & DISPOSAL

Facilities and Work Areas

- Ensure that facilities and work areas containing PHI are secure
- Ensure that anyone entering a controlled area scans their badge
- Do not allow anyone to follow you or “piggy back” into an area without swiping their access badge

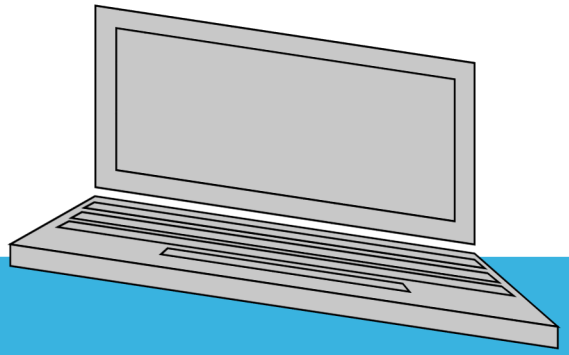
Storage and Disposal

- 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 laptop is lost or stolen, the loss must be immediately reported to the Service Desk. An investigation will be conducted to determine the risk of the data and potential use of the data in violation of HIPAA regulations
- To avoid theft of company equipment all employees should demonstrate appropriate judgment in safeguarding not only the physical property of the company, but the confidential information stored on the computer, or phone

INTEGRATED
HOME CARE SERVICES



WORK AREA INSTRUCTIONS

- 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 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 & 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 employment actions including warnings, termination and fines
- Monetary penalties 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 <u>all</u> of the following:**

- Disciplinary action for the company and the individual
- Personal criminal penalties
- Up to 10 years in prison
- Personal fines up to $250,000
- Sanctions against Integrated and increased scrutiny

BREACH

- All privacy and security incidents involving PHI need to be investigated.
- Employees/Contractors 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 MUST be completed if you suspect a breach has occurred.

YOUR RESPONSIBILITIES

- 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 Compliance Team or your HR Generalist
- Inform a 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
  - Compliance Hotline 954-381-7954 or
  - compliance@ihcscorp.com
- Insurance Administration Services (IAS)
  - compliance@Ihcscorp.com
  - Compliance Fax line 844-215-4265
  - HIPAA, Complaints and Fraud referrals via compliance@ihcscorp.com

SUMMARY

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

Following is a review of the key points covered in this training:

- HIPAA requires Integrated to keep PHI private and secure for our 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 Integrated and our employees/contractors
- Integrated employees/contractors are required to understand and comply with Integrated policies and procedures as they relate to HIPAA and the handling of PHI
- Integrated employees/contractors have a responsibility and obligation to identify and report suspected privacy and security incidents and violations


INTEGRATED
HOME CARE SERVICES