HIPAA ACKNOWLEDGMENT TRAINING

PATRIOT HOSPICE AND PATRIOT PALLIATIVE EMPLOYEES

CREATED BY: ERIC HOLLIDAY, MICHAEL DUNAGAN

WHAT IS HIPAA?

Acronym for **Health Insurance Portability & Accountability Act** of 1996 (45 C.F.R. parts 160 & 164).

Provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

HIPAA PRIVACY RULE

Privacy Rule went into effect April 14, 2003.

Privacy refers to protection of an individual's health care data.

Defines how patient information is used and disclosed.

Gives patients privacy rights and more control over their own health information.

Outlines ways to safeguard **Protected Health Information (PHI).**

HIPAA SECURITY RULE

Security (IT) regulations went into effect April 21, 2005.

Security means controlling:

- **Confidentiality** of electronic protected health information (ePHI).
- **Storage** of electronic protected health information (ePHI)
- **Access** into electronic information

HIPAA ELECTRONIC DATA EXCHANGE

Defines transfer format of electronic information between providers and payers to carry out financial or administrative activities related to health care.

Information includes coding, billing and insurance verification.

Goal of using the same formats is to ultimately make billing process more efficient.

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

(PHI) is any individually identifiable health information that is related to the past, present, or future of the following:

- **Physical or mental health** or condition of an individual
- **Provision of health care** to an individual
- **Payment** for the provision of health care to an individual
- **Patient Identifiers**

WHAT ARE PATIENT IDENTIFIERS?

PHI includes information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Examples:

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification numbers
- Vehicle Identifiers/Serial numbers/License plate numbers
- Internet protocol addresses
- Health plan numbers
- Full face photographic images and any comparable images
- Web universal resource locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

HIPAA REGULATIONS

HIPAA Regulations require we protect our patients' PHI in all media including, but not limited to, PHI created, stored, or transmitted through any of the following:

- **Verbal Discussions** (i.e. in person or on the phone)
- **Written on paper** (i.e. chart, progress notes, encounter forms, prescriptions, x-ray orders, referral forms and explanation of benefit (EOBs) forms)
- **Computer Applications and Systems** (i.e. electronic health record (EHR), Practice Management, Lab and X-Ray)
- **Computer Hardware/Equipment** (i.e. PCs, laptops, PDAs, pagers, fax machines, servers and cell phones)

HOW ARE THE HIPAA REGULATIONS ENFORCED?

The Public. The public is educated about their privacy rights and will not tolerate violations! They will take action.

Office For Civil Rights (OCR). The agency that enforces the privacy regulations providing guidance and monitoring compliance.

Department of Justice (DOJ). Agency involved in criminal privacy violations. Provides fines, penalties and imprisonment to offenders.

WHO OR WHAT PROTECTS PHI?

DOJ protects PHI through HIPAA regulations

Civil penalties up to $1,500,000/year for identical types of violations.

Criminal penalties:

- **$50,000** fine and **1 year prison** for knowingly obtaining and wrongfully sharing information.
- **$100,000** fine and **5 years prison** for obtaining and disclosing through false pretenses.
- **$250,000** fine and **10 years prison** for obtaining and disclosing for commercial advantage, personal gain, or malicious harm.

Our organization, through the **Notice of Privacy Practices** or **(NPP)**.

You, by following our policies and procedures.

WHY COMPLY WITH HIPAA?

To show our commitment to protecting privacy

As an employee, you are obligated to comply with **PH HEALTCARE** privacy and security policies and procedures

Our patients/members are placing their trust in us to preserve the privacy of their most sensitive and personal information

Compliance is not an option, it is required.

If you choose not to follow the rules:

- You could be put at risk, including **PERSONAL PENALTIES** and sanctions
- You could put **PH HEALTCARE** at risk, including financial and reputational harm

HIPAA SECURITY RULE

In general, the HIPAA Security Rule requires covered entities and business associates to do the following:

- **Implement administrative, physical, and technical safeguards** that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is created, received, maintained or transmitted.
- **Protect against any reasonably anticipated threats** or hazards to the security or integrity of ePHI.
- **Protect against any reasonably anticipated uses or disclosures** of ePHI that are not permitted or required under the Privacy Rule.
- **Ensure compliance** with security by its workforce.

HOW WE APPLY THE SECURITY RULE

Administrative Safeguards

Policies and procedures are **REQUIRED** and must be followed by employees to maintain security. (i.e. disaster, internet and e-mail use)

Policies and Procedures

Internet Use

- Access only trusted, approved sites.
- Contact the IT Department if you are redirected to any suspicious sites or if you notice any changes to websites that are critical to your job function.

E-Mail

- Keep e-mail content professional.
- Verify e-mail address before sending.
- **DO NOT** open e-mails or attachments if you are suspicious of or don't know the sender.
- **DO NOT** use a personal email address to send or receive any confidential information.
- Include a Confidentiality Disclaimer Statement in the Signature of all emails.

HOW WE APPLY THE SECURITY RULE

Technical Safeguards

Technical devices needed to maintain security.

- Assignment of different levels of access
- Screen savers
- Devices to scan ID badges
- Audit trails
- Network Firewalls

Physical Safeguards

Must have physical barriers and devices:

- Lock doors
- Monitor visitors
- Secure unattended computers

ACCESS TO EPHI

Information Access Management

PH Healthcare must implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the HIPAA Security Rule.

User Names

PH Healthcare must assign a unique name and/or number for identifying and tracking user identity. It enables an entity to hold users accountable for functions performed on information systems with ePHI when logged into those systems.

ACCESS TO EPHI

Passwords

The Security Rule requires PH Healthcare to implement procedures regarding access controls, which can include the creation and use of passwords, to verify that a person or entity seeking access to ePHI is the one claimed.

The use of a strong password to protect access to ePHI is an appropriate and expected risk management strategy which can be implemented by the following:

- Use at least 6-8 characters
- Use a mix of Capital and Lowercase Letters along with Numbers and Symbols
- Use a “pass-phrase” such as MbcFi2yo (My brown cat Fluffy is two years old)
- **DO NOT** use passwords that others may be able to guess (Spouse’s Name, Pet or Child’s Name, Significant Dates, Favorite Sports Teams)

AUDIT CONTROLS

The Security Rule requires organizations to implement hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems that contain or use ePHI.

Organizations should define the reasons for establishing audit trail mechanisms and procedures for its electronic information systems that contain ePHI.

Reasons may include, but are not limited to:

- System troubleshooting
- Policy enforcement
- Compliance with the Security Rule
- Mitigating risk of security incidents
- Monitoring workforce member activities and actions

PHYSICAL SECURITY

How can I help protect our offices and facilities?

- **Wear your ID Badge at all times** (helps identify you as a PH Healthcare employee/provider).
- **Only let employees enter** through employee entrances with you.
- **Keep hallway doors closed** that lead to patient care areas.
- **Request vendors and contracted individuals to sign-in** and obtain Vendor ID Badges when visiting a restricted area.

WHAT ARE RESTRICTED AREAS?

Restricted areas are those areas within our offices and facilities where PHI and/or organizationally sensitive information is stored or utilized such as:

- Receptionist stations/desks
- Medical Records Office
- Patient care hallways/treatment areas
- Administrative Offices(Accounting, Billing, HR, IT, Nursing, etc.)
- Storage/Network closets and cabinets
- Employee work rooms/areas
- Areas containing potential safety hazards

SAFEGUARDING PHI PAPER

How should I handle paperwork that contains confidential information?

- Turn over/cover PHI when a coworker approaches you to discuss something other than that PHI.
- Turn over/cover PHI when you leave your desk/work area so others cannot read it. (If you have an office, you have the option of closing your door instead)
- At the end of the day, place all papers containing PHI in an approved secure location.(Medical Records Office, Lockable File Drawer, Lockable File Cabinet, etc.)
- **DO NOT take pictures of PHI** to send in email or text messages.(If you need to send PHI, either scan to folder on printer or fax the information to the destination)

How should I dispose of confidential paper?

Shred or place all confidential paper in the designated confidential paper bins.

SAFEGUARDING PHI
FAX

What should I know when transmitting PHI via Fax?

Only fax information when in best interest of patient care or payment of claims.

Faxing sensitive PHI, such as mental health and STD's is strongly discouraged.

Check Fax Machine often to ensure that PHI is not left out to the public eye.

It is best practice to test a fax number prior to transmitting information. If this is not possible:

- Restate the fax number to the individual providing it.
- Obtain telephone number to contact the recipient with any questions.
- Do not include PHI on the cover sheet.
- Verify you are including only correct patient's information (i.e. check the top and bottom pages).
- Double check the fax number prior to transmission

SAFEGUARDING PHI COMPUTERS/PHONES

What rules should I follow when accessing PHI via Desktop or Laptop Computer?

- Restrict viewing access to others
- Lock your Computer when not in use by pressing the Windows Key + L
- **DO NOT** add your own software
- **DO NOT** modify or delete any software that is already installed on your computer
- **DO NOT** save PHI to the computer without prior authorization
- **DO NOT** save passwords to Network Folders, VPN(s), or any Website that contains PHI/access to PHI
- **DO NOT** write passwords on Sticky Notes to adhere to computer/monitor

What rules should I follow when using Smartphones provided by PH Healthcare?

- Use a 6 digit pin code
- **DO NOT** add personal email to device
- **DO NOT** save passwords or PHI in notes app

HIPAA VIOLATIONS

Incidental

If reasonable steps are taken to safeguard a patient's information and a visitor happens to overhear or see PHI that you are using, you will not be liable for that disclosure.

- Incidental disclosures are going to happen (even in the best of circumstances).
- Disciplinary action for incidental disclosure will typically be a verbal warning, re-education, and review/signing of the Confidentiality Agreement. Actual action taken against employee will be determined by a collaboration of Privacy Officer(s), Director of Human Resources and the Department Manager.

Accidental

Mistakes happen. If you mistakenly disclose PHI or provide confidential information to an unauthorized person or if you breach the security of confidential data, you must

- Acknowledge the mistake and notify your supervisor and the Privacy Officer(s) immediately.
- Learn from the error and help revise procedures (when necessary) to prevent it from happening again.
- Assist in correcting the error only as requested by your leader or the Privacy Officer. Don't cover up or try to make it "right" by yourself.

HIPAA VIOLATIONS

Intentional

If you ignore the rules and carelessly or deliberately use or disclose protected health or confidential information, you can expect:

- Disciplinary action, up to and including termination
- Civil and/or criminal charges

Examples of Intentional Violations of Privacy Include:

- Accessing PHI for purposes other than assigned job responsibilities
- Attempting to learn or use another person's access information

RISK ASSESSMENT FACTOR #1

Evaluate the nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification of the PHI.

- Social Security Number
- Credit Card Number
- Financial Data
- Clinical Details
- Diagnosis
- Treatment
- Medications
- Mental Health
- Substance Abuse
- Sexually Transmitted Diseases
- Pregnancy

RISK ASSESSMENT FACTOR #2

Consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made.

- Does the unauthorized person who received the information have obligations to protect its privacy and security?
- Is that person workforce of a covered entity or a business associate?
- Does the unauthorized person who received the PHI have the wherewithal to re-identify it?

RISK ASSESSMENT FACTOR #3

Consider whether the PHI was actually acquired or viewed or if only the opportunity existed for the information to be acquired or viewed.

- Laptop computer was stolen, later recovered and IT analysis shows that PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised
- The entity could determine the information was not actually acquired by an unauthorized individual, although opportunity existed

RISK ASSESSMENT FACTOR #4

Consider the extent to which the risk to the PHI has been mitigated.

- Obtain the recipient's satisfactory assurance that information will not be further used or disclosed through a Confidentiality Agreement, Reasonable Assurance, or Credible means of Destruction.

REPORTING HIPAA VIOLATIONS

If you are aware or suspicious of an accidental or intentional HIPAA violation, it is your responsibility to report it.

- So they can be investigated, managed, and documented
- So they can be prevented from happening again in the future
- So damages can be kept to a minimum
- To minimize your personal risk
- In some instances, management may have to notify affected parties of lost, stolen, or compromised data

PH Healthcare may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone who in good faith reports a violation (whistleblowing).

- Refer to the **http://hhs.gov** for more information, FAQs, and examples on what to report.

WHY IS PRIVACY AND SECURITY TRAINING IMPORTANT?

It is **everyone's responsibility** to take the confidentiality of patient information seriously.

Anytime you come in contact with patient information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations.

The law requires **HIPAA** Training be available for all employees.

To ensure your understanding of the **Privacy and Security Rules** as they relate to your job.

HIPAA AND YOUR ROLE

Remember, it is your responsibility, as a PH Healthcare employee or provider, to comply with all privacy and security laws, regulations, and PH Healthcare policies pertaining to them.

Employees and providers suspected of violating a privacy or security law, regulation, or PH Healthcare policy are provided reasonable opportunity to explain their actions.

Violations of any law, regulation, and/or PH Healthcare policy will result in disciplinary action, up to and including termination.