By: Millard, Lindsey M

HIPAA TRAINING COURSE

2020 Version

Welcome to the HIPAA Training.

Welcome to the HIPAA Training.

Table of Contents

[HIPAA Training Outline **Error! Bookmark not defined.**](#_Toc49181797)

[**Module 1 Introduction** 3](#_Toc49181798)

[What is HIPAA? 3](#_Toc49181799)

[Three Key Aspects of Compliance 3](#_Toc49181800)

[What does it mean to be “HIPAA Compliant”? 3](#_Toc49181801)

[HIPAA Background 4](#_Toc49181802)

[**Module 2 HIPAA Definitions** 4](#_Toc49181803)

[Introduction 4](#_Toc49181804)

[Health Information Definition 4](#_Toc49181805)

[Defining Protected Health Information (PHI) 4](#_Toc49181806)

[Covered Entity Definition 5](#_Toc49181807)

[Business Associate Definition 6](#_Toc49181808)

[BAs and HIPAA Rules 6](#_Toc49181809)

[Hybrid Entity Definition 6](#_Toc49181810)

[Quiz Question 6](#_Toc49181811)

[**Module 3 Privacy Rule** 7](#_Toc49181812)

[**Introduction** 7](#_Toc49181813)

[Minimum Necessary Uses 7](#_Toc49181814)

[Permitted Disclosures 7](#_Toc49181815)

[Uses and Disclosures for Treatment and Payments 8](#_Toc49181816)

[Incidental Disclosures 8](#_Toc49181817)

[**Definition of an Allowable Incidental Disclosure** 8](#_Toc49181818)

[Authorizations 9](#_Toc49181819)

[Authorization for the Release of Information 9](#_Toc49181820)

[Content of Authorization 9](#_Toc49181821)

[When Is Authorization Needed? 9](#_Toc49181822)

[Quiz Questions 9](#_Toc49181823)

[**Module 4 Security Rule** 10](#_Toc49181824)

[**Introduction** 10](#_Toc49181825)

[What Will We Cover? 10](#_Toc49181826)

[Technical Safeguards to Preventing an Attack 11](#_Toc49181827)

[What is Encryption? 11](#_Toc49181828)

[County Encryption 11](#_Toc49181829)

[Ramsey County Password Standard 11](#_Toc49181830)

[Password 11](#_Toc49181831)

[Physical Safeguards to Preventing an Attack 12](#_Toc49181832)

[Administrative Safeguards to Preventing an Attack 12](#_Toc49181833)

[Password Strength Requirements 13](#_Toc49181834)

[Minimum Requirements 13](#_Toc49181835)

[DO NOT: 13](#_Toc49181836)

[**Module 5 Individual Privacy Rights** 14](#_Toc49181837)

[Notice of Privacy Practices (NPP) 14](#_Toc49181838)

[**Introduction** 14](#_Toc49181839)

[Acknowledgment of Notice of Privacy Practices 14](#_Toc49181840)

[What the Notice Tells Patients- Verify this is on HHS Site 14](#_Toc49181841)

[Acknowledgment by Patient -Verify this is on HHS Site 14](#_Toc49181842)

[Patient and Provider Rights - Verify this is on HHS Site 15](#_Toc49181843)

[Individual Privacy Rights 15](#_Toc49181844)

[Penalties for Non-Compliance 15](#_Toc49181845)

[Penalty Guidelines 15](#_Toc49181846)

[Additional CE Penalties 16](#_Toc49181847)

[Where to go with HIPAA questions? (Need to add content) 16](#_Toc49181848)

[**HIPAA KNOWLEDGE CHECK QUESTIONS** 17](#_Toc49181849)

[Answer Key 19](#_Toc49181850)

Add Introduction video – add closed caption.

# **Module 1**

## **Introduction**

Welcome to the HIPAA Training.

In this training, we will learn about three basic concepts related to what it means to be HIPAA compliant. In addition, we will learn about what is protected by HIPAA.

# What is HIPAA?

HIPAA stands for the **Health Insurance Portability and Accountability Act.** It is a federal law that protects the privacy and security of health information.

The **Federal Department of Health and Human**

**Services,** also known as HHS, created three rules found in the Code of Federal Regulations or CFR that are part of HIPAA.

These rules are:

* Privacy Rule
* Security Rule
* Individual Privacy Right

We will discuss in detail the three general statements on what it means to be HIPAA compliant on the next slide.

# Three Key Aspects of Compliance

* **Privacy** - HIPAA compliance is a privacy issue first. It allows Protected Health Information to be shared in limited circumstances. HIPAA privacy regulations apply regardless of the format of the data.
* **Information Security** - HIPAA compliance involves law and technology. The HIPAA Security rule lays out the minimum IT and physical security standards
* **Individual Privacy Rights** - HIPAA not only protects privacy data, it gives individuals rights regarding how their private data is used, shared and accessed.

# What does it mean to be “HIPAA Compliant”?

Being compliant requires ongoing efforts and is a dynamic process. Organizations and their employees must first achieve compliance and then must maintain their level of HIPAA compliance by ensuring that daily activity is performed within HIPAA’s privacy and security guidelines. HIPAA compliance can be measured by audits or other reviews.

**Add statement- That says in order to be HIPPA compliant Ramsey must provide annual training.**

## **Quiz Questions**

# HIPAA Background

**HIPAA** was enacted as a broad Congressional attempt at healthcare reform - it was initially introduced in Congress as the Kennedy-Kassebaum Bill.

The landmark Act was passed in 1996 with two objectives. One was to ensure that individuals would be able to maintain their health insurance between jobs.

1. One was to ensure that individuals would be able to maintain their health insurance between jobs.  This is the Health Insurance Portability part of the Act.  It is relatively straightforward, and has been successfully implemented.
2. The second part of the Act is the "Accountability" portion.  This section is designed to ensure the security and confidentiality of patient information/data.  In addition, it mandates uniform standards for electronic data transmission of administrative and financial data relating to patient health information.

# **Module 2 HIPAA Definitions**

## **Introduction**

In this section will cover the most common term of HIPAA. Let’s review what they are;

## Health Information Definition

“**Health Information"** means any information in any form regarding an individual’s medical condition, the provision of their medical care, or the payment for their medical care that is created by an entity subject to HIPAA.

**“Protected health information”** has a two-part definition:

* an **individual identifier** (like a person's name or social security number)
* and **health information** about the individual.

## Defining Protected Health Information (PHI)

**Protect Health Information -** "Protected health information means individually identifiable health information:

* **General Definition :**
* Information that identifies an individual and describes his/her medical condition or treatment
* **Specifically Includes:**
* Clinical information
* Information on Payment
* Basic Demographic Information
* Name, Address, and Telephone Number
* **Includes Physical or Electronic Information**
* Healthcare Services

## Covered Entity Definition

**What is a Covered Entity?**

**Covered Entities** are defined in the HIPAA rules as;

1. Health Plans
2. Health Care Clearinghouses
3. Health Care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

**Examples of a Cover Entity listed below;**

|  |  |  |
| --- | --- | --- |
| Health Plans | Health Care Clearinghouses | Health Care Providers |
| This includes;   * Health Insurance Companies * HMO’s * Company Health Plans * Government programs that pay for health care, such as Medicare, Medicaid, and the Military and Veterans health care programs. | This includes;   * Clearinghouses are essentially electronic stations or hubs that allow healthcare practices to transmit electronic claims to insurance carriers in a secure way that protects Patient Health Information, or protected Health Information. | This includes providers such as;   * Doctors * Clinics * Psychologists * Nursing Homes * Pharmacies |

**The HIPAA Rules apply to Covered Entities and Business Associates**.

Individuals, organizations, and agencies that meet the definition of a **Covered Entity** under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

If a covered entity engages a **Business Associate** to help it carry out its activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules’ requirements to protect the privacy and security of protected health information.

In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules.

## Business Associate Definition

A **Business Associate** is defined as a person or company that creates, receives, or transmits Protected Health Information on behalf of a covered entity.

A Business Associate does notwork directly for the covered entity as a permanent employee or in the capacity as a member of the covered entity's workforce.

## BAs and HIPAA Rules

The list is very broad and covers many types of activity. For example, consulting, legal, management, and administrative services can be performed by a Business Associate.

The list also includes **subcontractors** that create, receive, maintain, or transmit Protected Health Information on behalf of a Business Associate.

In other words, a company or person that works for a Business Associate as a subcontractor would be a Business Associate.

## Hybrid Entity Definition

**Hybrid Entity** –  A HIPAA Hybrid Entity is a single legal organization that has some functions covered by HIPAA and some that are not. Ramsey County is a HIPAA hybrid entity. As a result, not every part of the county needs to comply with HIPAA.

The county designates which departments are covered by HIPAA in the HIPAA Healthcare Component table, posted on RamseyNet. Add a real link to RamseyNet.

So much for the legal definition; let’s break that down a little. A covered entity means a company that offers some health care-related services and some non-health care-related services. A covered function means anything that would render the performer a health plan, health care provider, or health care clearing house.

The list also includes **subcontractors** that create, receive, maintain, or transmit Protected Health Information on behalf of a Business Associate.

In other words, a company or person that works for a Business Associate as a subcontractor would be a Business Associate.

## **Quiz Question**

**Which of these is not a Covered Entity?**

A) Health Plan

B) Healthcare Provider

C) Healthcare Clearinghouse

D) Financial Consultant

# **Module 3 Privacy Rule**

## **Introduction**

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

## Minimum Necessary Uses

The **"Minimum Necessary"** dictates that employees should only access the "minimum necessary" amount of PHI, to perform their job functions. This regulates whether an employee can access PHI, including the amount, and type of PHI.

Ramsey County must authorize access to PHI in accordance with the Privacy and Security Rules. Employees should be restricted to accessing only the amount of PHI necessary to perform their jobs.

Once an employee is granted access to a system containing PHI, they may only access the records necessary to do their job. And, systems containing PHI should track which staff members access which records to ensure only the minimum necessary is accessed.

**For example**, a child and teen checkups nurse can access PHI about a patient she treated, but should not be granted access to PHI belonging to patients in other areas of the county.

## Permitted Disclosures

HIPAA Privacy Rule: Permitted PHI uses and Disclosures

**To the Individual** – A HIPAA covered entity may disclose protected health information to the individual who is the subject of the information.

**Treatment, Payment, and Health Care Operations** – A covered entity may use and disclose PHI for its own treatment, payment, and health care operations activities. Other disclosures include provider treatment and payment activities.

Another option is obtaining consent – written permission from individuals to use and disclose their PHI for treatment, payment, and health care operations. Consent is optional under the Privacy Rule for all covered entities.

**A covered entity may use and disclose PHI for its own treatment**, payment, and health care operations activities.

# Uses and Disclosures for Treatment and Payments

The **HIPAA** Privacy Rule permits a health care provider to **disclose** protected health information about an individual, without the individual's authorization, to another health care provider for that provider's **treatment or payment** purposes, as well as to another covered entity for certain health care operations such as….

**Health Care Operations include:**

* Maintenance of medical records
* Maintenance of accounting records
* Quality assurance activities
* Staff credentialing and performance evaluation
* Conducting financial and management audits
* Investigating complaints
* Supporting legal activities
* Resolving grievances

## Incidental Disclosures

The HIPAA Privacy Rule is not intended to impede patient care and therefore does not mandate that all risk of these incidental disclosures be removed to maintain compliance. Instead, the HIPAA Privacy Rule allows for certain incidental disclosures protected health information (PHI) when a Covered Entity is maintaining all other elements of compliance, including necessary safeguards and policies and procedures that reflect the [minimum necessary standard](https://gazelleconsulting.org/hipaa-minimum-necessary-standard/) to privacy.

### **Definition of an Allowable Incidental Disclosure**

The [HHS defines](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html) an incidental disclosure as the following:

*“An* ***Incidental*** *use or* ***Disclosure*** *is a secondary use or* ***disclosure*** *that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or* ***disclosure*** *that is* ***permitted*** *by the Rule.*

*However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.”*

**Examples of incidental disclosure**

* An overheard conversation among staff members
* An overheard discussion between staff and patients
* An overheard telephone call to a patient
* Test results filed in patient records

**Incidental Disclosures are permitted** ... but should be avoided:

* Incidental disclosures need not be documented

**Try to minimize incidental disclosures!**

* Conduct discussions in private areas, remember a hallway is not private.
* Limit discussion when others are present

# Authorizations

The HIPAA [Privacy Rule](https://compliancy-group.com/hipaa-basics/) requires that an individual provide signed authorization to a [covered entity](https://compliancy-group.com/hipaa-compliance-for-covered-entities/), before the entity may use or disclose certain protected health information (PHI).

Under the Privacy Rule and in accordance with the [minimum standards](https://compliancy-group.com/the-hipaa-minimum-necessary-standard/), doctors, nurses, hospitals, laboratory technicians, and other health care providers that are covered entities may use or disclose PHI (e.g.,  protected health information, X-rays, laboratory and pathology reports, diagnoses, and other medical information) *without the patient’s authorization*, for *treatment purposes*.

A HIPAA authorization form gives covered entities permission to use protected health information for purposes *other than*treatment, payment, or health care operations.

## Authorization for the Release of Information

Required for uses and disclosures of PHI other than for:

* + Treatment
  + Payment
  + Health care operations
  + To comply with legal mandates

Signed by the patient or patient’s personal representative

## Content of Authorization

Authorization must:

* Identify the information to be used or disclosed
* Identify users/persons to whom disclosed
* Authorization generally cannot be a requirement for treatment
* Note that it may be redisclosed by others

Cannot withhold treatment for authorization

* Treatment requested by the patient for disclosure

## When Is Authorization Needed?

Marketing:

* Promoting third-party products/services
* Providing mailing lists to others
* Any marketing when financial remuneration is provided to the practice

To use or disclose PHI other than:

* For treatment, payment, health care operations
* To comply with legal mandates
* General business management

Staff may use and disclose only the *minimum necessary* information.

## **Quiz Questions**

# **Module 4 Security Rule**

## **Introduction**

The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity.

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

It is important to understand simple do's and don'ts related to working with Protected Health Information (PHI) and the HIPAA Security.

**The HIPAA rules define a "Workforce Member" as an...**

* Employee
* Volunteer
* Trainee
* Any other person that performs work...

...for a Covered Entity (CE), or Business Associate (BA), under the direct control of the CE or BA, even if the workforce member does not receive pay.

CE's and BA's may be fined for a HIPAA violation for the "act or omission" of a workforce member, such as for failing to implement reasonable security safeguards.

This training provides information on safeguarding PHI related to HIPAA Security Rule.

Remember, **your employer must sanction workforce members who fail to comply** with your organization's policies and procedures, including safeguards.

## What Will We Cover?

* Safeguards to Prevent an Attack
* Knowing if your workstation is “Under Attack
* Using Local Email versus Web Mail
* Understanding “Social Engineering”
* The Dangers of Internet Browsing

# Technical Safeguards to Preventing an Attack

These security standards address safeguards that must be in place to protect infrastructure that can access, handle, or store electronic protected health information (PHI).

Examples include having anti-virus software, data encryption, and firewalls. These measures protect your networks and devices from data breaches.

* Encrypt sensitive files that your organization sends via email and ensure that any cloud-based platform you use offers encryption.
* Protect your network from hackers and other cyberthieves with firewalls and intrusion detection and prevention systems.
* Train your employees to identify and avoid phishing scams.
* Require that employees periodically change their passwords, and ensure passwords contain a mix of letters, numbers, and special characters.
* Keep updated documentation of your organization’s technology and network configurations.

Maintaining compliance requires monitoring changes in the law and upgrading outdated technologies.

What is Encryption? Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of a type of formula.

County Encryption – Ramsey County encrypted email should be used by staff who must use email to transmit private, confidential or other nonpublic data outside the Ramsey County network. Recipients will receive a message from Microsoft with instructions for how to retrieve their encrypted message.

## Ramsey County Password Standard

Passwords ensure that only approved individuals can access Ramsey County's technology systems and assets.  However, passwords have serious weaknesses as an access control. For high-risk systems, other approved authentication methods that provide greater levels of assurance and accountability may be used to in place of passwords.

## Password

**To Manage or prevent attacks, a user will:**

- Change his or her password every 90 days.

- Use a password different than the previous 24 passwords.

# Physical Safeguards to Preventing an Attack

These security standards address safeguards that must be in place to protect the physical premises of an organization.

Examples include having locks on doors, placing screen protectors on computers, and ensuring that papers containing protected health information (PHI) are not publicly viewable.

These HIPAA rules help your organization prevent [physical theft](https://www.insureon.com/blog/ways-to-prevent-burglary-theft-at-your-business) and loss of devices that contain patient information. Listed below are few examples safeguards measures.

* Limit access to computers by keeping them behind counters, secured to desks, and away from the general public.
* Restrict access to secure areas, monitor building safety, and require visitors to sign in.
* Exercise caution and follow best practices when upgrading or disposing of hardware and software, including securely wiping hard drives.
* Train employees and contractors on physical safety best practices, including the importance of securing their cell phones and mobile devices.

# Administrative Safeguards to Preventing an Attack

These security standards address safeguards that must be in place to guide staff on the actions they should take to maintain the security and integrity of PHI.

A variety of security measures are provided behind the scenes at Ramsey County, such as hard drive encryption and automatic deployment to workstations and servers of anti-virus software, security patching and software updates. Access to other services and systems may be governed by business need or security policies.

* Formalize your privacy procedures in a written document.
* Ramsey create the ethics and compliance office to oversee data security and HIPAA compliance.
* Identify which employees have access to data.
* Train employees on your organization’s privacy policy and how it applies to their job.
* Require all outside parties who need to access protected data to sign contracts stating that they will comply with HIPAA security rules.
* Back up data and have an [emergency plan for disasters](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.insureon.com%2Finsurance-glossary%2Fdisaster-recovery-plan&data=02%7C01%7Clisa.markham%40CO.RAMSEY.MN.US%7C72867a17abe1449d633e08d8460d40d6%7Cc073ebb35b56471386cf555efc97f68f%7C0%7C0%7C637336370014404688&sdata=4esyh9JRI7xEwm8pcPAe%2FVWZjq5GaFWKYfuYDxw907c%3D&reserved=0) that could cause information loss.
* Perform an annual data security assessment.
* Create a data breach response plan that addresses notifying affected patients and fixing compromised IT systems.

## Password Strength Requirements

**HIPAA** regulations **require** healthcare entities to enact procedures for creating, **changing**, and safeguarding passwords, but they don't specify the details or the required complexity of the passwords.

Increasing password complexity helps prevent unauthorized access to your account. Ramsey implemented technology that detects passwords that are weak or previously involved in a break. Weak passwords are easily guessable, contain seasons, days, years and common names. Anything discoverable about you on social media should not be used as a password.

### Minimum Requirements

A password **WILL** be:

* At least twelve (12) or more characters.
* A mix of alpha and numeric, with at least one digit (0 through 9) or special character ($, @. # and so on).
* Made up of at least one Uppercase and one lowercase character.
* More complex than a single word (such passwords are easier for hackers to crack).

### DO NOT:

- Disclose your password to anyone, including county management and technical support staff, even if they demand it.

* + - **If this happens, you must escalate to your line management immediately**.
* The only exception is disclosure to a law enforcement officer in accordance with local laws. In this circumstance, seek guidance from the county's legal department.

- Use a password on any county systems that are used on external systems (including Internet banking and social networking services).

- Write down your password.

- Use the "remember password" feature in any Web browser.

- Use any "password keeper", programmable device, or "password wallet" software or service.

## **Quiz Questions**

# **Module 5 Individual Privacy Rights**

## Notice of Privacy Practices (NPP)

## **Introduction**

When you mention HIPAA, most people reference the **Notice of Privacy Practices (NPP)** they received at the hospital, doctor’s, dentist’s or eye doctor’s office.

The **NPP** is a document that tells your patients, employees, or clients how their health information may be used and shared and lists their health **privacy rights** related to Protected Health Information (PHI).

It's a part of the HIPAA **Privacy** Rule and a key requirement for the organization.

## Acknowledgment of Notice of Privacy Practices

HIPAA law requires doctors, hospitals, or other healthcare providers to **keep records that clients or employees have received the notice**.

You may do this by getting a signature acknowledging the individual received the NPP or keeping a dated log of NPP distribution.

* **Notice of Privacy Practices**:

A statement given to each patient describing how the practice will use and disclose health information and outlining the patient's rights under HIPAA.

* **Acknowledgment:**

Written documentation that the notice was provided to a patient, either signed by the patient or completed by a staff member explaining why the patient did not sign it.

## What the Notice Tells Patients

* How their information will be used
* With whom their information will be shared
* When an authorization is needed
* How to request an accounting of uses and disclosures
* How to request access to information
* How to request changes in information

## Acknowledgment by Patient

* Staff must try to obtain acknowledgment
* Document that the notice was given
* Required on first visit only
* Obtain before treatment
* Use of acknowledgment form Patient signature and date
* Document attempt if patient can’t acknowledge
* Emergency treatment exception
* Patient gets a copy of the acknowledgment

## Patient and Provider Rights

HIPAA gives patients certain rights:

* To review and copy their records
* To request changes in their records
* To have changes communicated to others

HIPAA gives providers certain rights

* To charge for copies of health information
* To deny requested changes in patient records
* Staff credentialing and performance evaluation
* Conducting financial and management audits
* Investigating complaints
* Supporting legal activities
* Resolving grievances

# Individual Privacy Rights

The **HIPAA Privacy Rule** (the **Privacy Rule**) provides **individuals** with a legal, enforceable **right** to see and receive copies upon request of the information in their medical and other health records maintained by their health care providers and health plans.

The Privacy Rule generally requires HIPAA covered entities (health plans and most health care providers) to provide individuals, upon request, with access to the protected health information (PHI) about them in one or more “designated record sets” maintained by or for the covered entity.

This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual’s choice.

Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.).

# Penalties for Non-Compliance

The Security Rule establishes a set of national standards for confidentiality, integrity and availability of e-PHI. The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

## Penalty Guidelines

The Federal Department of Health and Human Services (HHS) may impose a fine on a CE or BA if HHS determines that the CE or BA violated the HIPAA rules.

## Additional CE Penalties

A CE may also be liable for, a HIPAA violation committed by an agent, workforce member, or a business associate of that CE, who is working for the CE. A “work force member” means an employee, trainee, volunteer or other person whose work is under the direct control of the CE.

# Where to go with HIPAA questions? (Need to add content)

## **Quiz Question**

## Summary Wrap Up.

# HIPAA KNOWLEDGE CHECK QUESTIONS

1. **The primary federal law pertaining to medical information privacy is:**

* American Recovery and Reinvestment Act (ARRA)
* **Health Insurance Portability and Accountability Act (HIPAA)**
* Health Information Technology for Economic and Clinical Health Act
* All of the above
* None of the above

1. **What is PHI?** 
   * Protected Health Identifier
   * Patient Health Insurance
   * **Protected Health Information**
   * Privacy Health Information
2. **HIPAA is needed for:**

* **Protection of personal health information and our rights with respect to that information and to prevent fraud abuse.**
* Ability to provide health insurance to everyone and cut the cost of insurance.
* Improvement of the economy in the Unites States and to eliminate the need for health care insurance.
  + Prevention of infections and to lower the cost of prescription.
  + Drugs
  + None of the above

1. **Protected Health Information, PHI can include which of the following:** 
   1. Name
   2. Date of birth
   3. Medical record number
   4. Message or issue
   5. Diagnosis
   6. Admission date, time and reason
   7. **All of the above**
2. **The HIPAA Privacy Rule protects all PHI, electronic, verbal and written.** 
   1. **True**
   2. False
3. **My responsibility under HIPAA includes:** 
   1. Handling PHI as if it were my own
   2. Disposing of scrap paper and other documents with PHI by shredding or confidential disposal
   3. Accessing PHI, only the minimum necessary, to do my job
   4. Discussing potential violations or any HIPAA concerns with my supervisor, manager or the designated HIPAA Privacy/Security Official
   5. **All of the above**
4. **What is a privacy breach?** 
   1. A team member fails to maintain confidentiality by discussing patient health information on social media
   2. Lab results are sent to the wrong patient or recipient
   3. A laptop or Smartphone containing electronic PHI is lost or stolen – and the device is not encrypted
   4. A computer hacker gains access to systems that contain PHI
   5. **All of the above**
   6. None of the above
5. **An example of a Business Associate of a HIPAA covered entity is:** 
   1. An answering service
   2. A contractor providing IT services and support
   3. A transcription service
   4. Collection and billing vendors
   5. **All of the above**
6. **If you need to report a HIPAA concern or violation, which of the following can you do?** 
   1. Contact my supervisor or manager
   2. Contact my HIPAA Site Coordinator
   3. Contact my organization’s HIPAA Compliance Officer
   4. **All of the above**

# Answer Key

1. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
2. PROTECTED HEALTH INFORMATION
3. PROTECTION OF PERSONAL HEALTH INFORMATION AND OUR RIGHTS WITH RESPECT TO THAT INFORMATION AND TO PREVENT FRAUD AND ABUSE
4. ALL OF THE ABOVE
5. TRUE
6. ALL OF THE ABOVE
7. ALL OF THE ABOVE
8. ALL OF THE ABOVE
9. ALL OF THE ABOVE