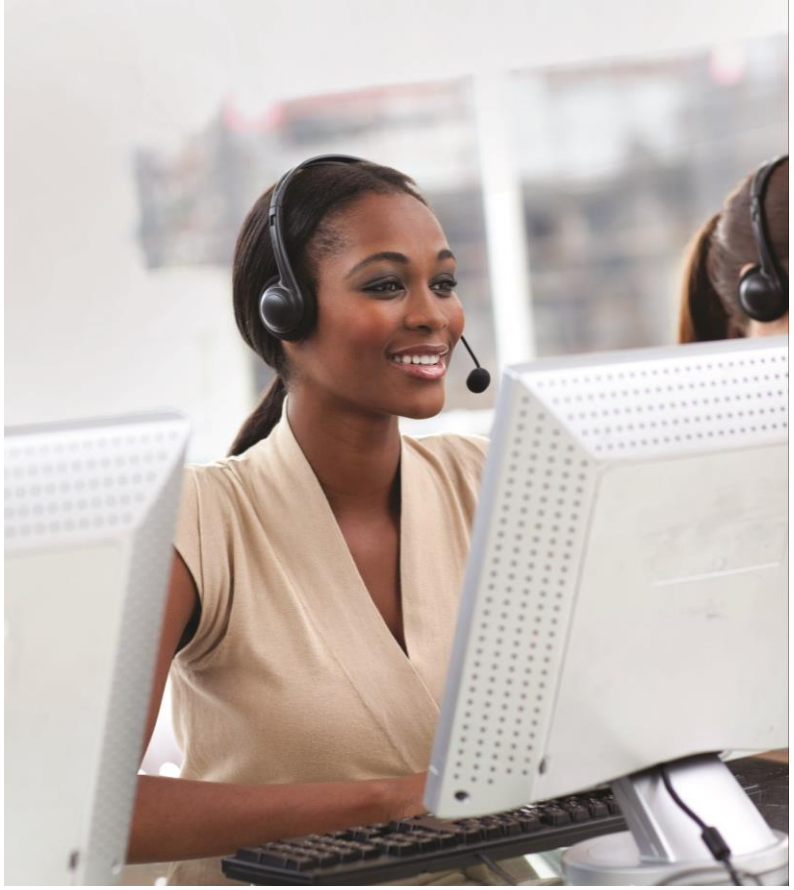


# HIPAA COMPLIANCE TRAINING

LIBERTY DENTAL PLAN®

# WHAT IS HIPAA?

## Health Insurance Portability & Accountability Act

**HIPAA is a federal law enacted to:**

1. Protect the privacy of a member's personal and health information
2. Provide for the physical and electronic security of personal health information
3. Simplify billing and other transactions with Standardized Code Sets and Transactions
4. Specify new rights of members to approve access/use of their medical information

# THE BREAKDOWN OF HIPAA

## H I P A A

- Health Insurance Reform (Portability)
- Administrative Simplification (Accountability)
- HITECH

The HIPAA Privacy Rule – explains how to use, manage and protect personal or protected health information (PHI or ePHI).

# WHAT IS THE HITECH ACT?

## *Health Information Technology for Economic and Clinical Health*

**The HITECH Act acts as an addendum HIPAA, giving the U.S. Department of Health and Human Services (HHS) broader jurisdiction to penalize medical practices for not securely handling personal health information (PHI).**

- **Applies to all electronic "unsecured PHI"**
- **Requires immediate notification to the Federal Government if more than 500 individuals are effected**
- **Requires an annual notification if less than 500 individuals are affected**
- **Requires notification to a major media outlets**
- **Breach will be listed on a public website**
- **Requires individual notification to members**
- **Criminal penalties apply to individuals or employees of a covered entity**
- **Increased enforcement & fines for breaches**

# REQUIREMENTS FOR HIPAA

To protect the **privacy *and* security** of an individual's Protected Health Information (PHI)

To require the use of only **minimally required necessary information**

To extend the **rights of individuals** over the use of their PHI

# THE HIPAA PRIVACY RULE

**The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by LIBERTY, in any form or medium, whether electronic, on paper, or oral. The Privacy Rule calls this information *protected health information* (PHI).**

**Protected health information is information, including demographic information, which relates to:**

- An individual's past, present, or future physical or mental health or condition,
- A provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

# WORKING WITH PHI

**Protected health information (PHI) includes many common identifiers, such as:**

1. **Names**
2. **All geographical subdivisions smaller than a State**, including **street address, city**, county, precinct, **zip code**, and their equivalent geocodes
3. **Dates** (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
4. **Phone numbers**
5. **Fax numbers**
6. **E-mail addresses**
7. **Social Security numbers**
8. **Medical record numbers**
9. **Health plan beneficiary numbers**
10. **Account numbers/Member Numbers**
11. **Certificate/license numbers**
12. **Vehicle identifiers and serial numbers, including license plate numbers;**
13. **Device identifiers and serial numbers;**
14. **Web Uniform Resource Locators (URLs)**
15. **Internet Protocol (IP) address numbers**
16. **Biometric identifiers, including finger, retinal and voice prints**
17. **Full face photographic images and any comparable images Ex. X-rays**
18. **Any other unique identifying number, characteristic, or code** *(note this does not mean the unique code assigned by the investigator to code the data)*

# MINIMUM NECESSARY STANDARD

**Protected health information should not be used or be disclosed when it is not necessary to satisfy a particular purpose or to carry out a function.**

**Examples:**

- **Never put PHI in the subject line of e-mail;**
- **Only provide information necessary to fulfill a specific request/purpose** Example - don't circulate an entire medical record, if only eligibility dates requested
- **Keep distribution of PHI to only those minimally necessary –** Example - don't include PHI on emails or correspondence with large distribution groups (many people copied)
- **Redact PHI when not necessary to fulfill request –** Example - if department needs a copy of claim to validate total amount billed, redact all PHI not related to the request such as diagnosis; DOB, address, etc. Ask first, if you are not sure.

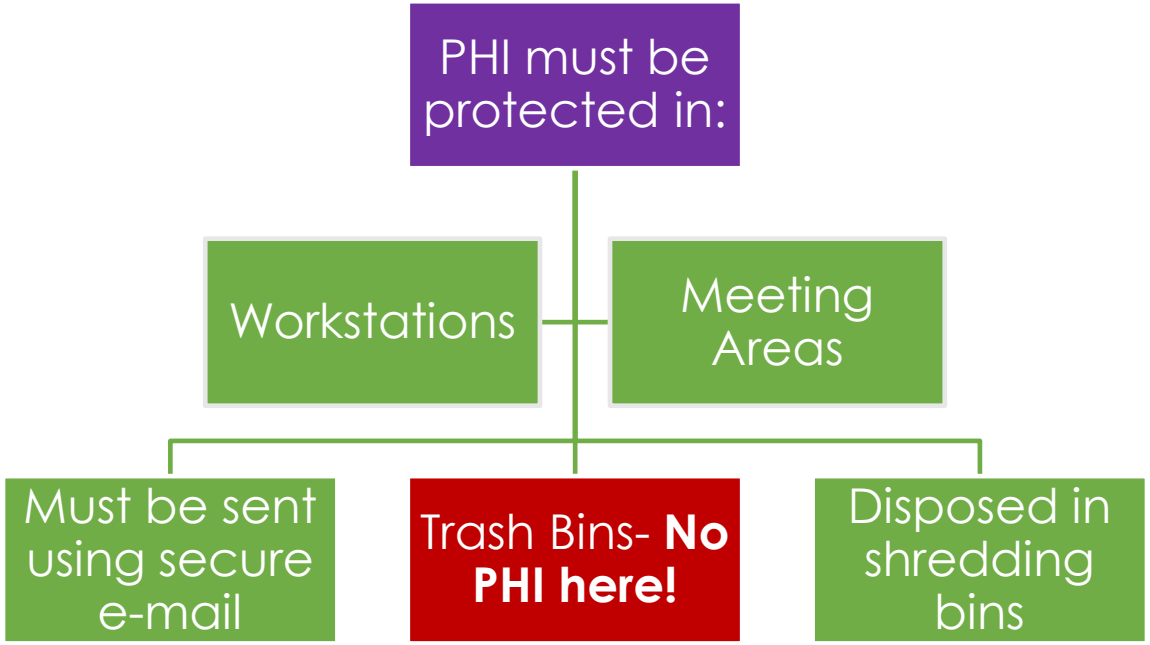
# PRIVACY AND SECURITY CONCERNS

- **Theft** of member Data
  - Identity Theft
  - Stolen laptop
- **Loss** of member Data
  - Incorrect disposal
  - USB Drives
- **Misuse** of member Data
- **Misdirected** email, fax, or data transfers

# PROTECTING OUR MEMBER'S INFORMATION:

**We must protect an individual's personal, financial and health information that:**

- Is created, received, or maintained by a health care provider or health plan
- Is written, spoken, or electronic
- Includes at least one of the 18 personal identifiers in association with health information



# USE GOOD COMPUTING SKILLS!

| | |
|---|---|
| Lock your screen | **Use Windows+L** |
| Computer Security | ***Save PHI to H drive only*** |
| Workstation Security | ***Follow the clean desk policy*** |
| Anti-Virus | ***Run all required updates!*** |
| Report Security Incidents | |

# IMPORTANT REMINDER

When exposed to PHI, you should only share, use or verify PHI when required for treatment, payment or healthcare operations, or when permitted or required by law.

# VERBAL AWARENESS

**Members can be concerned about:**

- Being asked to state out loud certain types of confidential or personal information
- Overhearing conversations about PHI by staff performing their job duties
- Being asked about their private information in a "loud voice" in public areas

## Protecting Privacy: Verbal Exchanges

Members may see normal operations as violating their privacy *(incidental disclosure)*

*Ask yourself: "What if it was my information being discussed in this place or in this manner?"*

## Incidental disclosures and HIPAA

***"Incidental": a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure. §164.502(c)(l)(iii)***

***Incidental disclosures are permitted if there is reasonable and important intentions. This may be commonly misunderstood by members!***

**Members have the right to:**

- Make a complaint
- Receive an accounting of any external releases
- Obtain a paper copy of the Notice of Privacy Practices on request
- Request restrictions on release of their PHI
- Receive confidential communications
- Inspect and copy medical records (access)
- Request amendment to medical records

# USE OR DISCLOSURE OF HEALTH INFORMATION

**Written** authorization is required to release health information

**Dentists may share information** with a referring dentist regarding "members in common" without an authorization

**All emergency requests** for health information should be documented in the member's medical record.

The Health and Human Services (HHS) Office for Civil Rights assigns breaches to one of five different categories:

1. Hacking/IT incidents- most frequent cause!
2. Unauthorized access/disclosures
3. Theft
4. Loss
5. Improper disposal

# CAUSES OF HEALTHCARE DATA BREACHES

# HIPAA VIOLATIONS CAN CARRY PENALTIES!

**Criminal and Civil Penalties:**

- Monetary fines
- Jail Terms up to 10 years

**Fines & Penalties - Violation of State Law**

- Staff may be fined per violation and reported to their licensing board if applicable

**LIBERTY Corrective & Disciplinary Action**

- Up to & including loss of privileges and job loss

# HIPAA IN THE NEWS

- "A popular health insurer sent two mailings to its members in which highly sensitive information relating to HIV and Afib diagnoses was visible through the windows of the envelopes. The case was settled for $935,000." **(HIPAA Journal)** This affected close to 2,000 CA residents.
- "An ambulance company was investigated over the reported loss of an unencrypted laptop computer that contained the PHI of 500 patients. OCR found there had been a risk analysis failure, there was no security awareness training program for staff, and HIPAA Security Rule policies and procedures had not been implemented. The case was settled for $65,000." **(HIPAA Journal)**
- "A civil monetary penalty of $1,600,000 was imposed on Texas Department of Aging and Disability Services for multiple violations of HIPAA Rules discovered during the investigation of breach involving an exposed internal application. OCR discovered there had been risk analysis failures, access control failures, and information system activity monitoring failures, which contributed to the impermissible disclosure of 6,617 patients' ePHI."**(HIPAA Journal)**

# LET'S REVIEW!

- HIPAA and HITECH together establish the requirements for the use, disclosure, and safeguarding of individually identifiable health information.
- According to HIPAA, PHI that is linked to health information based on the 18 identifiers must be treated with special care.
- Not protecting PHI can result in civil and criminal penalties, fines, corrective and disciplinary action.
- Remember to use safe computing skills!