

# HIPAA Business Associate Training 2025



# Training Objectives

Upon completion of this training, you will be able to:

- ✓ Describe your responsibilities for protected information under HIPAA including reporting violations and consequences of violations
- ✓ Describe best practices for safeguarding confidential information
- ✓ Know how to contact DePaul's Privacy, Information Technology, and Compliance Staff

# What is **HIPAA**



A federal law designed to give individuals control of their personal information (Protected Health Information or PHI), to allow communication among providers, and to protect and ensure confidentiality of this information.

# Health Insurance Portability *and* Accountability Act



If you need access to Protected Health Information (PHI) in order to conduct your business with DePaul, you'll need to comply with Federal HIPAA Laws.



# Protected Health Information (PHI)

Any data that could identify persons being served by DePaul. This includes identifying individual information and program information as well as any information regarding physical or mental health conditions and includes spoken, written and electronic information.

## Examples of Identifying Information:

- ✓ Name
- ✓ Address
- ✓ Driver's License
- ✓ Social Security Number
- ✓ Email Address
- ✓ Date of Birth
- ✓ Demographic Information
- ✓ Phone Numbers
- ✓ Account Numbers
- ✓ Photos and videos
- ✓ Any information about a person's physical or mental health or services at DePaul



# How Does HIPAA Pertain to Vendors?

If you provide goods or services to DePaul which involve the use or disclosure of or, require access to protected health information (PHI) of individuals we serve you may be considered a “Business Associate” of DePaul.

As a Business Associate you will be required to Sign a Business Associate Agreement (BAA) with DePaul along with your other contract requirements

## **Examples of Business Associates can include:**

- IT vendors
- I Cloud providers,
- Consultants and service contractors
- Billing and record storage contractors



# Business Associate Overview

## **Direct Liability**

Business associates who handle PHI on behalf of covered entities are directly liable for HIPAA compliance.

## **Breach Notification:**

Business Associates need to know what constitutes a breach of PHI and the procedures for notifying the covered entity and potentially, individuals whose information was compromised.

## **Avoiding Penalties:**

Failure to comply with HIPAA can result in significant penalties for both covered entities and Business Associates



# Your Responsibilities Under HIPAA

As a Business Associate of DePaul, you are required to:

- Adhere to uses of protected health specified in your contract.
- Avoid using use or further disclosing the protected health information other than as permitted or required by your contract or as required by law;
- Use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
- Follow all Federal HIPPA regulations pertaining to Business Associates

# The Following HIPAA Rules Apply to Business Associates



## **HIPAA Privacy Rule:**

- This rule protects the privacy of PHI and outlines how it can and cannot be used or disclosed.

## **HIPAA Security Rule:**

- This rule focuses on protecting electronic protected health information (ePHI) and includes security standards for covered entities and business associates. You are responsible for data security, data integrity, and data access controls.

## **HIPAA Breach Notification Rule:**

In the case of a breach you must notify DePaul, individuals affected by the breach and the Secretary of HHS of certain breaches of unsecured PHI.





# Issues You Should Report

The following issues should be reported to DePaul's Corporate Compliance Officer, Privacy Officer or Security Officer immediately

## Loss of Information

- ❖ Loss or misplacement of confidential information such as **charts, record information, etc.**
- ❖ Loss or compromise of of **equipment** containing confidential information

## Misuse of Information or System Access

- ❖ Disclosure of confidential protected information to individuals who shouldn't have access whether accidental or unauthorized
- ❖ **Misdirected** faxes and mail

**Failure to report a violation is a violation!**

# Consequences of Not Complying With HIPAA

You could face fines and penalties including:

- x **Civil Penalties:** up to **\$50,000** per violation up to **\$1.5** million per incident for violations which are not corrected, per calendar year
- x **Criminal Penalties:** **\$50,000** to **\$250,000** in fines and up to **10 years in prison**

# If You Have a Question or Become Aware of a Privacy or Security Breach



***Contact the Compliance Officer, Security Officer, or Privacy Officer:***

**Lisa Corrigan**  
Compliance Officer  
(585) 719-3127  
lcorrigan@depaul.org

**Pat Cirillo**  
Privacy Officer  
(585) 719-3123  
pcirillo@depaul.org

**Chris Berson**  
VP, Chief Information Officer,  
Security Officer  
(585) 719-3163  
cberson@depaul.org

**Report anything suspicious or a suspected violation immediately**

## **HIPAA**

**Protecting PHI is your responsibility.**