Information Privacy & Security

Yasmin Andre

Associate Vice President of Compliance & Risk Management

United Way

Heart of Florida United Way

Training Objectives

- Understand individual role in protecting confidentiality
- Recognize PII and PHI
- Reasonably safeguard PII and PHI
- Prevent unauthorized disclosures
- Report confidentiality breaches

Important Notes

- This training **will not** replace the annual confidentiality training required of all Part B subcontracted providers.
- Attending this training will provide **one (1.0) credit hour** towards the 15-hour annual training requirements for all Part B case management staff.
- Confidentiality standards included in this training conform with the Florida Department of Health HIV Case Management Guidelines, Section 2 – Confidentiality and DOHP 50-10.
- For further reference:
  - FIPA (Florida Information Protection Act of 2014)
  - HIPAA (Health Insurance Portability Accountability Act)

Did You Know?

- The number of reported data breaches is increasing.
- As of 2023, 79.7 percent of data breaches were due to hacking incidents and ransomware attacks.
- The Office of Civil Rights posts a list of breaches affecting 500 or more individuals, known as the "Wall of Shame."
- The largest healthcare data breach occurred at Anthem Inc., in 2015 involving the records of 78.8 million people.
  - The recent Change Healthcare attack in February 2024 may yet break this record.

Know Your Role

Heart of Florida United Way

Who is Required to Do Confidentiality Training?

- All employees and volunteers with access to client information must receive annual training on confidentiality, the proper exchange of information, and required consent. Documentation of training must be maintained in personnel records.
- The Florida Department of Health HIV Section has written security policies, protocols, and procedures to ensure the security of information and to protect confidentiality, data integrity, and access to information in accordance with the Florida Statutes.
  - DOHP 50-10
- Providers may create their own security policies, protocols, and procedures; however, they must be consistent with DOHP 50-10.

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Why Do Confidentiality Training?

- The Florida Department of Health takes the privacy, security, and integrity of individuals' data seriously.
- Covered entities and business associates have legal responsibilities to protect PII and PHI, to identify and respond to suspected incidents, and to prevent harm.
- **Florida Department of Health Notifies Individuals Affected by June 2024 Cyberattack**
  - https://www.hipaajournal.com/ransomhub-florida-department-health-cyberattack/

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

What is My Role?

- It is every person's responsibility to know how to recognize PII/PHI and how to safeguard it from unauthorized access.
- Unauthorized disclosures of protected client information can result in significant harm to individuals.
- HIPAA violations carry individual and organizational financial and legal penalties, depending on the nature of the violation and the number of individuals impacted.
  - Ignorance of HIPAA Rules is no excuse for failing to comply with HIPAA Rules. In cases when a covered entity is discovered to committed a willful violation of HIPAA laws, the maximum fines may apply.

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

What are the HIPAA penalties?

Financial Penalties for HIPAA Violations:

Penalty Tier	Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of Knowledge	$137	$34,464	$34,464
Tier 2	Reasonable Cause	$1,379	$68,928	$137,886
Tier 3	Willful Neglect	$13,785	$68,928	$344,638
Tier 4	Willful neglect (not corrected within 30 days)	$68,928	$68,928	$2,067,813

Rates based on Notice of Enforcement Discretion (NED) issued in April 2019. Official OCR rates call for higher max penalty rate.

Criminal Penalties for HIPAA Violations:

Tier 1: Reasonable cause or no knowledge of violation – Up to 1 year in jail
Tier 2: Obtaining PHI under false pretenses – Up to 5 years in jail
Tier 3: Obtaining PHI for personal gain or with malicious intent – Up to 10 years in jail

United Way
Heart of Florida United Way

Recognizing PII and PHI

Heart of Florida United Way

Personal Identifiable Information

- The term "**PII**," has numerous official definitions.
- Simply put, it is any information that can be used to identify an individual directly or indirectly.
- PII can be used either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- **Sensitive PII (SPII)** is any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual.

Personal Identifiable Information

- Email
- Home Address
- IP Address
- Name
- Phone Number
- Any other information that can uniquely identify someone

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Sensitive PII

Stand-Alone

- Alien registration number
- Biometric identifiers
- Credit card number
- Driver's license or state ID number
- Financial account number
- Passport number
- Social Security number (SSN)

PII combined with the following

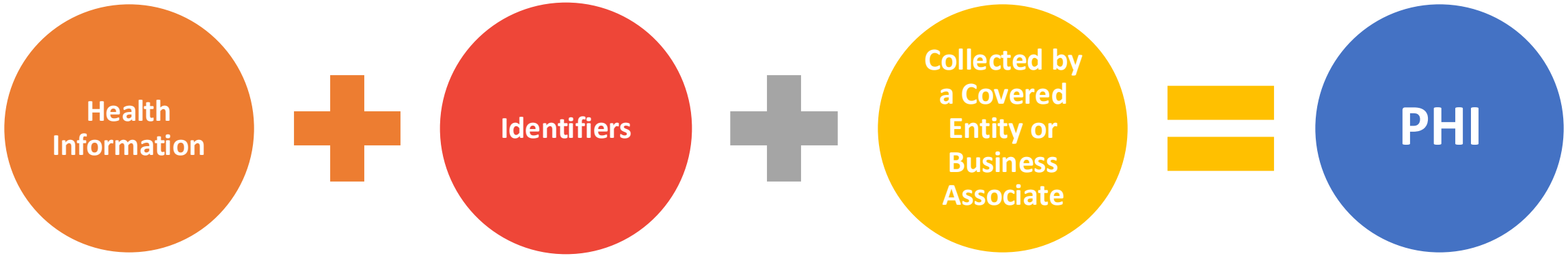
- Account passwords
- Citizenship or immigration status
- Criminal history
- Date of Birth (DOB)
- Last 4 digits of the SSN
- Mother's maiden name
- Ethnic or religious affiliation
- Medical information
- Personal financial information
- Sexual orientation

United Way
Heart of Florida United Way

Protected Health Information

- A special subset of PII is **protected health information**, or **PHI**.
- PHI carries the safeguarding requirements that apply to PII, plus additional safeguards as well.
- PHI includes any individually identifiable health information, such as a medical history or medical billing information, that was either created or received by a covered entity.
- Covered entities include health plans and almost all healthcare providers.

Personal Health Information



PHI – Health Information

- Allergies
- Medications
- Family medical history
- Health histories
- Health records
- Lab test results
- Medical bills
- Past, present, and future health conditions or physical/mental health
- Prognosis
- Treatment/Rehabilitation plans
- X-rays
- Any other information about a person's health

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

PHI - Identifiers

- Account numbers
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Certificate/license numbers
- Dates, except the year
- Device identifiers and serial numbers
- Email addresses
- Fax numbers
- Geographic data
- Full face photos and comparable images
- Internet protocol addresses
- Health plan beneficiary numbers
- Medical record numbers
- Names
- Social Security numbers
- Telephone numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Any unique identifying number or code

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

PHI – HIPAA Covered Entities

- Most health care providers - Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing homes, Pharmacies
- Health insurance companies
- HMOs (Health Maintenance Organizations)
- Employer-sponsored health plans
- Government programs that pay for health care - such as Medicare, Medicaid, and military and veterans' health programs
- Clearinghouses - organizations that process nonstandard health information to conform to standards for data content or format, or vice versa, on behalf of other organizations

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

PHI – Business Associates

- Data analysis, storage, and transmission services
- Legal and accounting services
- Billing and benefit management services
- Actuarial and claims processing services
- Any other businesses that perform activities that require them to have access to patient health information in order to provide services for or on behalf of health industry entities
- Examples: EMR systems, CAREWare, billing systems etc.

United Way
Heart of Florida United Way

Safeguarding PII/PHI

Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Reasonable Safeguards

- Sign a confidentiality agreement at least annually
- Using and disclosing only the ***minimum necessary*** for the purpose.
- Using ***encryption technology*** to protect sensitive PII and PHI.
- Enabling all available privacy settings.
- Ensuring that storage of any PHI by a vendor is only temporary.
- Ensuring that vendors do not use or disclose ePHI in a manner that is inconsistent with the HIPAA Rules.

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Secured Areas

- Designate & maintain secured areas for the security & privacy of information
- Provide appropriate access to information using administrative, physical & technical controls
- Access only provided to those members with documented **“need-to-know”** authorization

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

What is “Need to Know”

- Information provided to the person on the release should be on a “need to know” basis and be pertinent to the client’s care. “Need to know” is defined as:
  - The legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission.
  - The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.

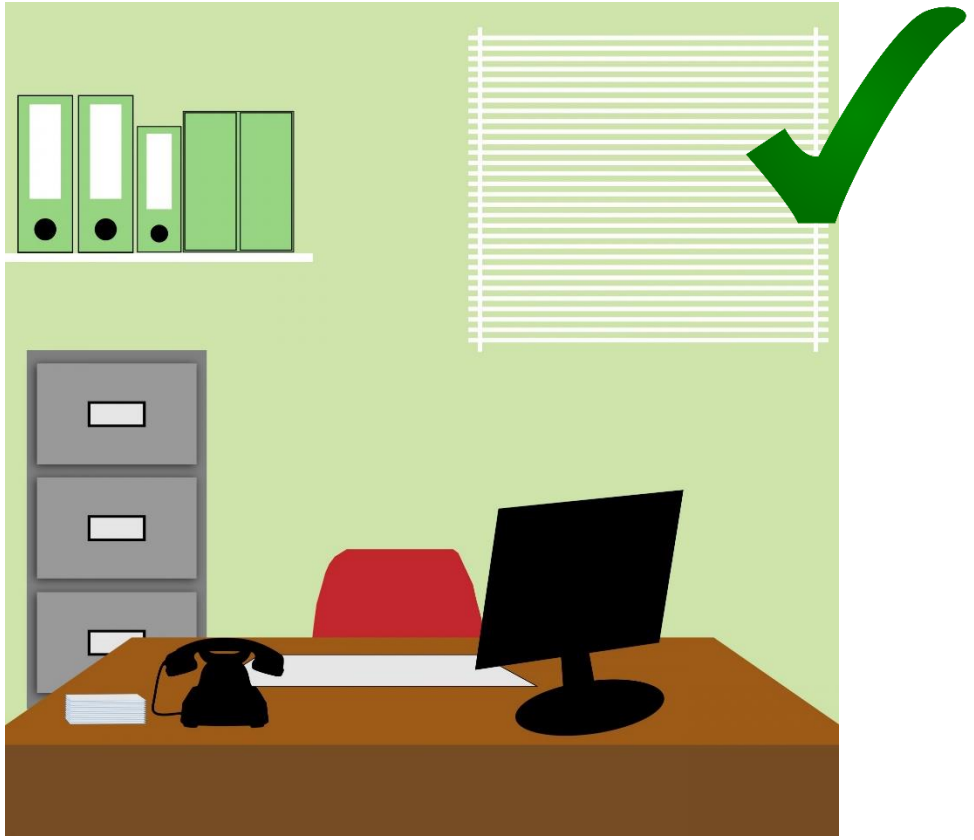
Physical Security

- Visitors must always be escorted
- Keep reliable locking systems
  - Double locked
- Access is limited to authorized staff
- Designate key custodians
- Keeping access logs

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Protecting Confidential Information

- Position computer monitors to prevent unauthorized viewing
- Designate people for file transfer
- Use encryption for electronic transmission
- Data back-ups must be locked in a secured area
- Do not use laptops to store information



United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Telephone Communication

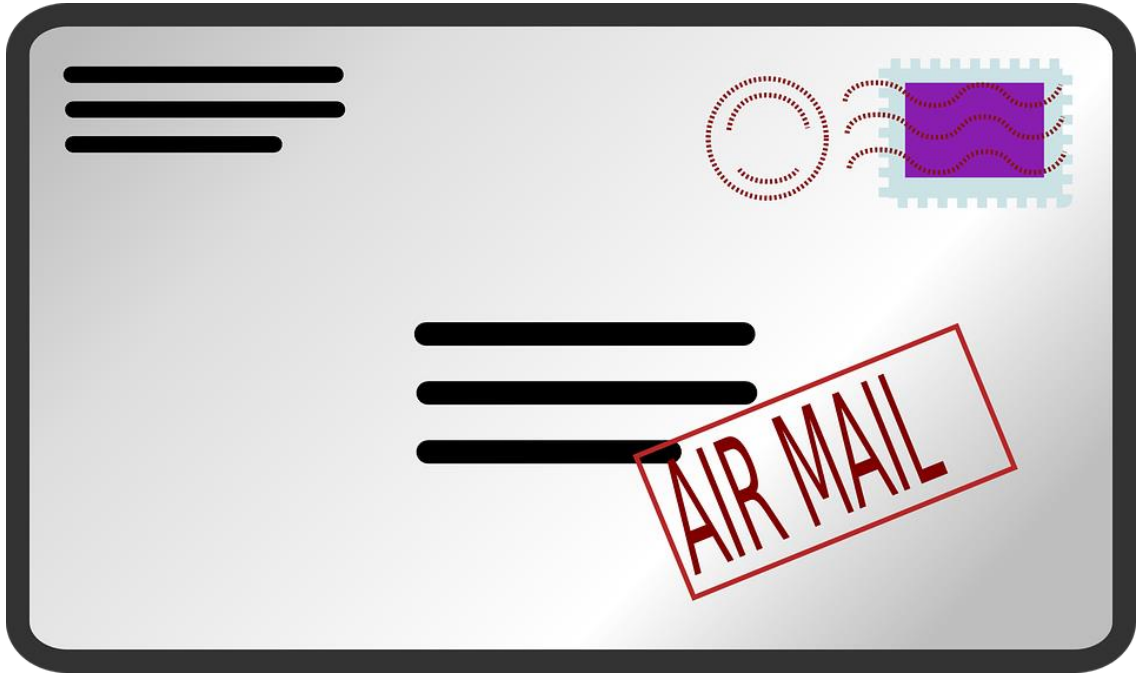
- Conduct conversations in private areas where they cannot be overheard
- Cell phones are NOT secure – advise the caller of cell phone use
- Determine caller identity before releasing any information
- Limit the information disclosed in a voicemail message

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Mailing Confidential Information

- Designate a secure mail intake to receive confidential information
- Mailrooms and mailboxes must be secured to prevent unauthorized access to incoming or outgoing mail
- Double envelope when mailing confidential information
  - Outside addressed to recipient
  - Inside marked confidential and specifies the recipient
  - Do not use specific program information or logos denoting HIV care



United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Faxing Confidential Information

- Keep fax machines in secured areas with limited visual access
- Before faxing, obtain consent & authorization to release the confidential information
- Generate activity report or call the recipient to confirm receipt
- Use a cover sheet marking the fax as “Confidential” – must include specific text

Medical information that is faxed must have a permanent copy in the record and documentation in the case notes.

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Confidential Fax Cover Sheet Sample

To:

Fax:

From:

Date:

Subject:

# of Pages Including Cover Sheet:

"This transmission may contain material that is CONFIDENTIAL under federal law and Florida Statutes and is intended to be delivered to only the named addressee. Unauthorized use of this information may be a violation of criminal statutes. If this information is received by anyone other than the named addressee, the recipient shall immediately notify the sender at the address or the telephone number above and obtain instruction as to the disposal thereof. Under no circumstances shall this material be shared, retained or copied by anyone other than the named addressee."

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

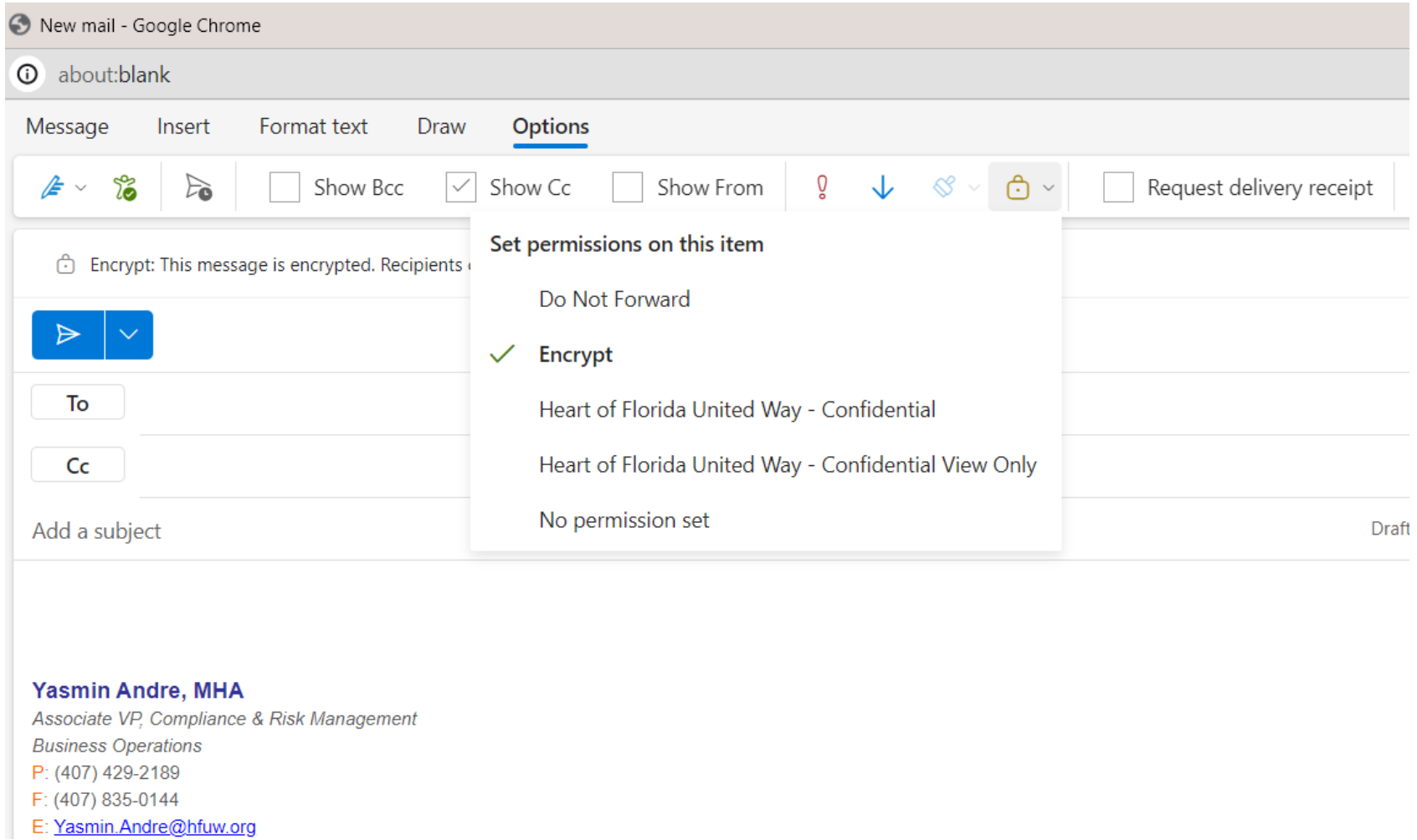
E-mail

- E-mail may be considered public record and archived
- Avoid emailing confidential information or replying to a client's email containing confidential information if possible
- E-mails containing confidential information **must be encrypted**, including any attachments

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Encrypting E-mail in Outlook 365



United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Off-Site Security & Data in Transit

- Confidential information should only be transported by persons authorized to do so in their position description and
  - must be secured using physical safeguards
  - not left unattended or in visible areas of a vehicle
  - must be tracked when taken into the field and signed out when removed from a secured area
  - limited to the minimum required to perform that day's responsibilities
  - returned by the close of the same business day
  - secured in a manner that does not risk disclosure

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Work Space

- Office space should allow for business to be conducted in a confidential manner
- If private office space with a door is not available, ensure all communications remain confidential
- Information with confidential identifiers should not be left unattended or unsecured
- Meetings involving confidential information must be held in areas with restricted access.
- Confidential information must be printed using appropriate technical and physical safeguards to prevent unauthorized viewing **– utilize private printing features**

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Storage of Information

- Offices and staff must maintain confidentiality of all data, files, and records, including client records related to services, and shall comply with state and federal laws, including but not limited to Sections 384.29, 392.65, and 456.057, F.S.
- Appropriate storage systems for hardcopy client records are required
- Appropriate storage systems for digital client records are required
- Storage systems must include, at a minimum, file folders that are kept in locked file cabinets (Double-locking required!)

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Client File Retention

- File retention must follow Florida Department of State Bureau of Archives and Records Management storage and disposition procedures as mandated in Chapters 119 and 257, F.S.
- Files must also be kept according to HRSA's client file retention policy.
- Follow your agency's Record Retention and Destruction policy
  - If a client file is closed, the file must be retained for a minimum of seven years before disposal
  - Documents must be disposed via certified shredding

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Electronic Files and Computers

- Computer monitors must be positioned to prevent unauthorized viewing
  - Use privacy screens
- All computers, including laptops, that access and store confidential information must be **password protected and encrypted**
- Laptops must be returned to the secured area at the end of the working day and never stored in an unsecured, unauthorized area
  - Do not store in the car, trunk, or home
- Deleting files from a computer hard drive is not sufficient when the device is no longer in use – hard drives must be wiped clean

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Additional Information

- Agencies need to document that positions have "need to know" access in their written job descriptions.
- All visitors to a restricted area must sign in on a security log.
- Unauthorized persons shall not be left unattended in areas where confidential or sensitive information is maintained.

United Way
Heart of Florida United Way

Preventing and Responding to Confidentiality Breaches

Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Most Common HIPAA Violations

Staff

- Snooping on Healthcare Records
- Unauthorized Disclosures of Protected Health Information
- Improper Disposal of PHI
- Insufficient ePHI Access Safeguards
- Failure to Use Encryption or an Equivalent Measure to Safeguard ePHI on Portable Devices

Organizational

- Failure to Perform an Organization-Wide Risk Analysis
- Failure to Manage Security Risks / Lack of a Risk Management Process
- Denying Patients' Access to Health Records/Exceeding Timescale for Providing Access
- Failure to Enter into a HIPAA-Compliant Business Associate Agreement
- Exceeding the 60-Day Deadline for Issuing Breach Notifications

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

How to Avoid Them

- Adopt a Clean Desk Policy and do not leave your workstation unlocked
- Use private print and do not leave files on copier tray
- Do not leave laptops unattended
- Store confidential information in approved electronic locations. **USB flash drives should not be used.**
- Schedule meetings or phone calls with clients in private areas (i.e. Private office/Conference Room)
- Enable encryption on email or use an approved system for protected file transfer

United Way
Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Accidental Violations

Any accidental HIPAA violation may qualify as a data breach and should be treated seriously to assess risk.

Examples of accidental violations include:

- Sending email containing PHI to the wrong recipient(s)
- Storing PHI insecurely or without a BAA
- Failing to obtain an authorization before disclosing records
- Disclosing more than the minimum necessary PII/PHI for a permitted use
- Sharing login credentials with colleagues

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Accidental Violations

- **See Something, Say Something!**
- **Report accidental or unknowing disclosures immediately**
  - To prevent future violations
  - To help us fill unknown gaps in compliancy
  - To minimize potential consequences or sanctions
- **An accidental disclosure is not a HIPAA violation in every case. Your agency and the DOH maintains procedures for breach determination.**

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

Handling Violations

- **If you receive an email or fax that is labeled confidential and intended for someone else, what should you do?**
  - Contact the sender and inform them of the mistake
  - Destroy or delete the communication without delay
  - Notify the sender that the communication was destroyed/deleted
- **What happens if someone accidentally, or unknowingly, violates HIPAA?**
  - Immediately report the error to a supervisor and your agency's Privacy Officer
  - Tell your colleague if they unknowingly violated HIPAA
- **What happens if there is a problem that compromises the security of our protected data, including PII/PHI?**
  - Immediately report the issue to your agency's Security Officer

Questions, Comments, Concerns

Heart of Florida United Way

UNITED WE FIGHT.
UNITED WE WIN.
LIVE UNITED

We want your feedback!

- Go to **www.menti.com** or scan the QR code
- Enter the code **6637 7066**

Heart of Florida United Way



Yasmin Andre

Associate VP, Compliance & Risk Management

Yasmin.Andre@hfuw.org

407-429-2189

United Way

Heart of Florida United Way