FairWarning®

Patient Privacy Monitoring System & Security Access

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

PHI is the information protected under the HIPAA regulation. It is created in a health care setting and contains 18 identifiers:

- NAME
- POSTAL ADDRESS
- ALL ELEMENTS OF DATES EXCEPT YEAR
- TELEPHONE NUMBER
- FAX NUMBER
- EMAIL ADDRESS
- URL ADDRESS
- IP ADDRESS
- SOCIAL SECURITY NUMBER
- VEHICLE IDENTIFIERS AND SERIAL NUMBER
- MEDICAL RECORD NUMBER
- HEALTH PLAN BENEFICIARY NUMBER
- DEVICE IDENTIFIERS AND THEIR SERIAL NUMBERS
- BIOMETRIC IDENTIFIERS (FINGER & VOICE PRINTS)
- FULL FACE PHOTO AND OTHER COMPARABLE IMAGES
- ANY OTHER UNIQUE IDENTIFYING NUMBER, CODE OR CHARACTERISTIC
- ACCOUNT NUMBER
- LICENSE NUMBER

PATIENT PRIVACY IN THE MEDICAL RECORD

HIPAA and the University allow access to a patient's medical record **ONLY** for **a business or clinical need**. Any access to patient information should relate to the **normal job functions of an employee**.

AS A UNIVERSITY OF MIAMI EMPLOYEE, PLEASE BE AWARE:

- You are **NOT** permitted to access your **own** healthcare information, except through the patient portal.
- You are **NOT** permitted to access the healthcare information of a **coworker**.
- You are **NOT** permitted to access the healthcare information of your **relatives** (spouse, children, parents, etc.).
- You are **NOT** permitted to access the healthcare information of **celebrities** or any other individual unless you have a specific, **job-related** need.

In an effort to maintain the integrity of the EHR, all systems containing sensitive information contain audit trails. Audit trails record **all user activity** including records accessed, dates and times of access, modifications made, printing, etc. Review of audit trails are routinely performed on University systems.

"BUSINESS OR CLINICAL NEED"

ACCESS TO PATIENT INFORMATION SHOULD BE FOR A LEGITIMATE CLINICAL, BUSINESS, RESEARCH OR EDUCATIONAL NEED **ONLY**. APPLY THIS ANALYTICAL TEST TO DETERMINE WHETHER IT IS PERMISSIBLE:

Is access to this record or this information required to complete my job?

Is this access necessary for Treatment, Payment or Healthcare Operations?

IF THE ANSWER TO EITHER OF THOSE QUESTIONS IS "NO", ACCESS WILL LIKELY BE INAPPROPRIATE. TALK TO A SUPERVISOR OR CALL THE PRIVACY OFFICE.

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

WHAT IS FAIRWARNING?

FairWarning® is an application that facilitates the automated monitoring of access to various Information Technology (IT) systems that house PHI (i.e. UChart) and identifies potentially inappropriate access behavior.

We audit because it is:

- An effective way to monitor the access of our employees to the systems housing PHI.
- Required under HIPAA to detect unauthorized access, use or disclosure.
- A way to be proactive versus reactive approach.
- A mechanism to investigate and respond to complaints.
- Assures the integrity of our system through responsible use of the EHR by employees.
- Proof, in a measurable way, that we take compliance seriously.
- Financially practical by helping us avoid fines.

A local health system was recently fined **$5.5 million** for failure to monitor.

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

WHAT IS THE PROCESS?

- The system generates an alert.
- The alert will be reviewed by FairWarning® and then again by the Privacy Office.
- Additional follow-up may be necessary to determine if the access was actually inappropriate (for a NON business or clinical purpose).

UHealth
UNIVERSITY OF MIAMI MILLER SCHOOL of MEDICINE

Memorandum

To: Sebastian Ibis

From: Office of Privacy and Data Security

Date: October 7, 2017

Subject: Inquiry/Concern - Electronic Health Record Access # FW (HS)

On October 1, 2017, **Jane Doe** (12345678) accessed the electronic health records of **John Doe** (EHR 4567890) in **UChart EMR**. A review of audit logs failed to identify a clinical or business related reason for the access. **Jane Doe** accessed Patient Selected from Patient Lookup, Visit Navigator template loaded, Data from related encounters accessed through VB, Report with patient data viewed, and SmartForm viewed.

You are identified as **Jane Doe**'s Supervisor. Please assist us in determining whether there was a clinical or business related reason for the access. Please review and complete the information below within ten (10) working days, no later than **November 1, 2017.** Memorandums not received within twenty (20) business days will be sent to the UMMG Executive Committee for review.

In the space provided, please explain steps taken to arrive at your determination. Additional pages and/or appropriate documentation should be included as needed.

☐ **No** – There is no clinical or business related reason for the access.

☐ **Yes** – There is a clinical or business reason for the access.

☐ **Unsure** – Clinical or business related reason for the access cannot be determined.

Please record actions taken related to the inquiry/concern. Additional pages and/or appropriate documentation should be included as needed.

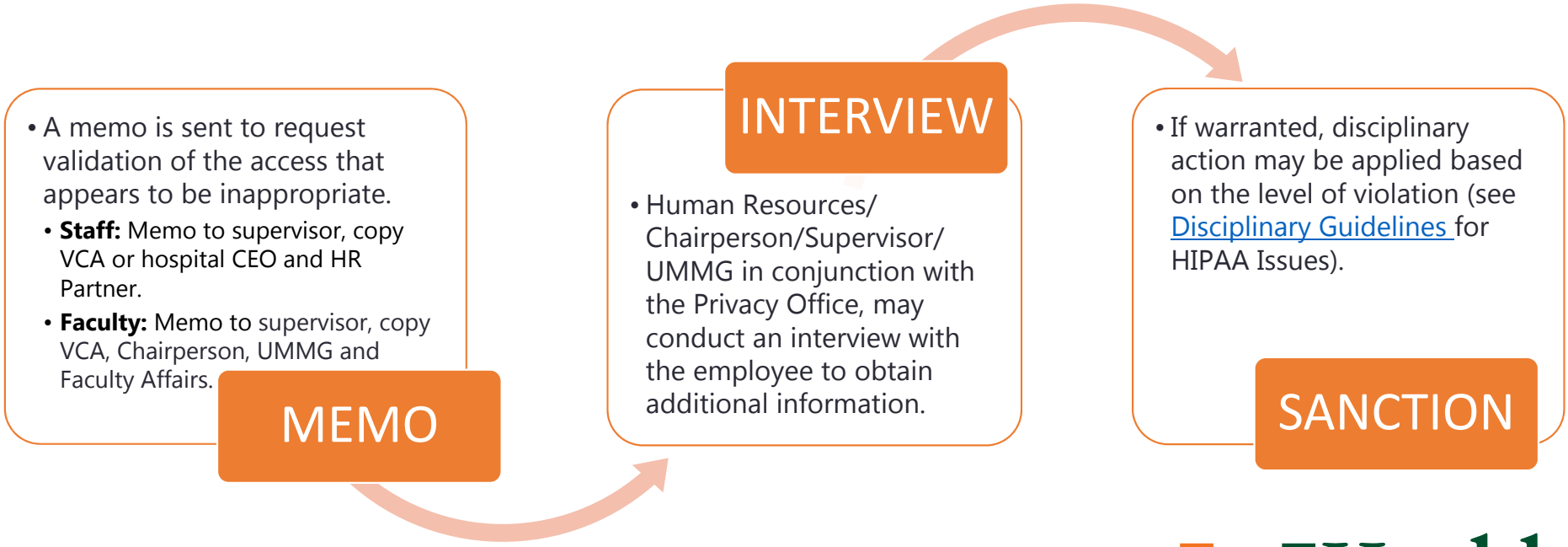
☐ **Review by Chair**
☐ **Meeting with Employee**
Participation: ☐ **Human Resources**
☐ **UMMG/Faculty Affairs**
☐ **Privacy Office**
☐ **Other** _____
☐ **Counseling/Education**
☐ **Provided by:** _____
☐ **Re-take CBL Training**
☐ **Training**
☐ **Disciplinary Action (Please provide details below)**
☐ **Termination**

CC: VCA
Faculty Affairs

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

WHAT IS THE PROCESS?

If an access appears to have been inappropriate (i.e., no apparent business or clinical need), then further investigation may include the following:



UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

WHY ACCESS FOR PERSONAL REASONS IS NOT APPROPRIATE

- Accessing a medical record inappropriately is a HIPAA violation!
- University policy dictates that the medical record be used for **business or clinical need only**. Access for personal use is a direct violation of policy and negatively impacts the integrity of the UHealth system.
- Treating medical personnel must be able to practice medicine without interference. **They should not feel like they have to censor themselves.**
- Physicians must have the flexibility and latitude to deliver news to patients, recommend follow-up testing, arrange services or interpret results in the context of the best interest of the patient.
- Access for self-treatment or treatment of family or friends raises issues related to medical ethics.
- Patients who are also physicians may not have fluency in a particular specialty or an adequate support system to deal with or interpret news when they discover it on their own.

Remember: When you seek treatment at the University of Miami, you are a patient (or the family member of a patient). Do not lose sight of your role as a patient and allow your medical practitioners to render treatment.

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

INAPPROPRIATE ACCESS: REAL CASES FROM THE PRIVACY OFFICE

Your **co-worker** had a procedure and you wanted to know the details.

You heard that **Mr. Celebrity** from your favorite show was seen a UHealth. You wonder what he came in for. **This type of access is generally the subject of huge breach fines.**

Your **spouse** had an x-ray and you want to see what the result was.

You want to look at **your own** chart to see at what time your next appointment is.

You need the new address of your **ex-spouse** to give to the attorney.

You allowed your **supervisor** to access records under **your credentials**.

Your **co-worker's** birthday is coming up but you can't remember the date and want to send out a card.

You are curious to see if your **sister's** surgery charge got resubmitted.

Your **neighbor** has an appointment and you want to know the doctors she is seeing and the reason.

You want to verify your **direct report's** appointment at UHealth for submission on Workday timesheets.

A **former employee** contacted you privately to verify their appointment.

You want to check the lab results for your **child**.

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

HOW DOES AN EMPLOYEE OBTAIN ACCESS APPROPRIATELY?

MyUHealthChart.com

If an employee needs access to their own health information:

- Access their information through the patient portal at MyUHealthChart.com.
- Access their child's information by completing the Child Proxy Access Form.
- Contact the hospital's Health Information Integrity office or the medical records custodian of the department or facility and complete the request for access form to obtain their records.

If an employee needs access to another adult's health information:

- The patient must authorize access by completing the Attachment 46, Third Party Authorization form.
- Complete the Adult Proxy Access Form (must be signed by the patient) to access another adult's information through MyUHealthChart.com.
- Contact the UChart Help Desk for assistance at askmyuhealthchart@med.miami.edu.

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

MOBILE DEVICES

Per University policy, personal smart phones, smart watches, tablets and other mobile devices may be used to access University email systems with certain conditions.

Employees must utilize the following security controls if they wish to access University email and other University applications:

- ✓ Require a PIN/password to restrict access. Change it often!
- ✓ Set your device to always require a PIN or password after 3 minutes or less of inactivity
- ✓ Enable "remote wipe"
- ✓ Keep operating system and applications up to date
- ✓ Encrypt all storage including data cards (SD, microSD, etc.)

TEXT MESSAGING

The use of text messaging to transmit PHI is **strictly prohibited**. While texting is a convenient way to communicate, it can lead to a variety of HIPAA violations for failure to adequately safeguard PHI.

- Phones may be lost or stolen and accessible by others.
- Messages may be intercepted, leaving senders with no control over their final destination.
- Messages can remain on wireless provider servers unauthorized by the University.
- Applications that claim to be HIPAA compliant or encrypted (such as WhatsApp) do not have an agreement with the University and thus are not permitted.

You may be faced with a situation in which you are asked to text message patient information by a supervisor, peer or even a patient. Decline and advise them to contact the Privacy Office with questions or concerns.

LAPTOPS AND PORTABLE STORAGE DEVICES (USB)

Encryption software is required for all laptops and portable storage devices (USB, external hard drive, etc.) that contain or will access PHI regardless of who owns the device.

- Laptops purchased or supplied by UMIT have pre-installed encryption.
- Personal laptops used for University business must have encryption installed and/or registered with UMIT.
- Any portable media device such as USB or portable hard drive that will store or secure PHI **MUST** be purchased with encryption.
- Encrypted devices, such as USBs, should be purchased from UMIT Procurement.

Tip: Store University information on Box rather than USB!

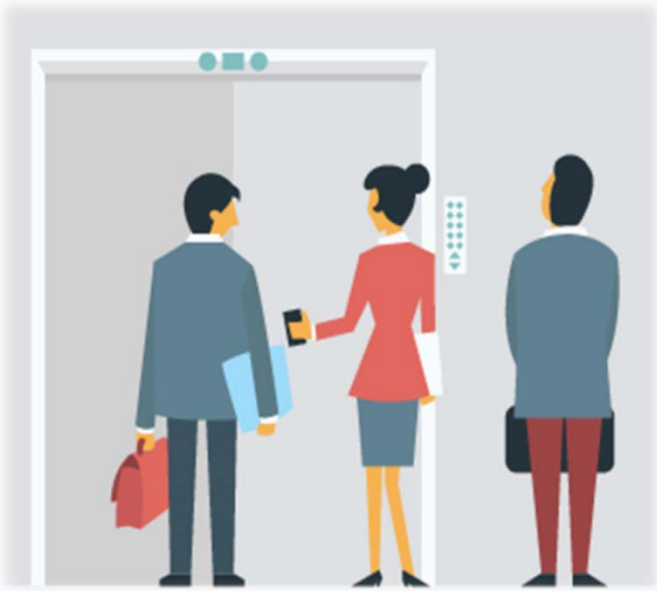
UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

PHYSICAL SAFEGUARDS

An important step in protecting PHI is to implement reasonable and appropriate physical safeguards for all systems, equipment and facilities. Common security controls are:

- ✓ **Personnel Controls:** Access controls such as appropriate use and safeguarding of ID badges and log-in information.
- ✓ **Property Controls:** Locked doors requiring ID badge entry for restricted areas; surveillance when appropriate.
- ✓ **Facility Access Controls:** Secure storage and proper disposal of sensitive information. Escort non-University personnel when visiting.
- ✓ **Device and Media Controls:** Use of privacy screens; secure storage of devices; lock or log off devices when stepping away.

BE AWARE OF YOUR SURROUNDINGS!



- Never take unauthorized photos of patients, their medical record or health data.
- Do not leave your mobile device unattended.
- Avoid having conversations about patients or PHI in public areas such as elevators.
  - Move confidential conversations to a private area.
- Be mindful of unauthorized individuals in secure areas.
- Ensure sensitive information is properly secured.
  - If you see unattended sensitive information on University property, remove it and notify the Privacy Office immediately.
- Use privacy screens in non-private areas.
- Lock or log off of devices before stepping away.

If you see something, say something!

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

RESOURCES

OFFICE OF PRIVACY & DATA SECURITY

- EMAIL: PRIVACY@MED.MIAMI.EDU
- PHONE: 305-243-5000
- WEBSITE: WWW.PRIVACY.MED.MIAMI.EDU

Onsite Training Available!

HIPAA
Research
FairWarning
...and more!

Helenemarie Blake-Leger, Esq., CIPP/US
Chief Privacy & Data Integrity Officer

Ishwar Ramsingh, MBA, CISSP, CIPM
Data Broker

Lisa M. Arenas, BSHA, CIPP/US
Director, Privacy & Security

Moises Jacobs, Esq.
Assistant Director, Privacy & Security

Tatiana L. Kulhanjian, MBA
Sr. Manager, Business Operations

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM