University Compliance, Ethics, and Risk Office

UNIVERSITY OF CENTRAL FLORIDA

University of Central Florida
Draft Policy Submission Cover Memo Form

Policy No. and Title: 2-013 HIPAA Compliance Policy and Manual

Initiating Authority: Vice President, People and Workplace Experience

Initiating Authority Approval Date: 2/18/2026

Date of Submission for Review: 4/28/2026

Submitted by: Director, Privacy Compliance

Department: Compliance and Ethics

☒ New Policy ☐ Existing Policy (5-year Review) ☐ Existing Policy (Out of Cycle Review)

Summary of Revisions: (For a new policy, please provide a summary of the policy. For an existing policy, please provide a summary of the revisions made to the policy.)

This policy establishes UCF's requirements for protecting the privacy and security of patient information in accordance with HIPAA and applicable state law. It applies to all UCF personnel and business associates involved with covered and non-covered healthcare units collectively known as the UCF Healthcare Component.

Stakeholders included in the Review Process: (Provide a list of departments involved in the review/revision process.)

The Division of People and Workplace Experience
Universtiy Ethics and Compliance
Privacy Compliance
HIPAA Collaborative

Stakeholder feedback must also be requested from the Faculty Senate and the College Policy Liaisons. By checking the boxes below, you are confirming that feedback from these groups was requested, received, and considered in the draft policy.

☒ College Policy Liaisons ☒ Faculty Senate

Regulatory Requirements (if applicable)**:** (Provide information on regulatory requirements pertaining to the policy, including specific statute or regulation number.)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
HIPAA Privacy Rule 45 CFR Part 160 adn subparts A and E of 164
HIPAA Security Rule 45 CFR Part 160 and subparts A and C of 164
HITECH Act (Health Information Technology for Economic and Clinical Health)
Florida Information Protection Act (FIPA)

Presenters: (Provide the name(s), position title(s), and email address(s) for all individuals who will be presenting the policy to the university's Policies and Procedures Committee.)

Kimberley Thrash, Director, Privacy Compliance
Christina Serra, AVP, Deputy Chief Compliance and Ethics Officer

Draft – HIPAA Compliance

Policy Number	2-013
Responsible Authority	Director, Privacy Compliance HIPAA Privacy and Security
Initiating Authority	Vice President, People and Workplace Experience
Effective Date	
Date of Origin	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all employees, students, residents, fellows, and volunteers who are employed by, or acting on behalf of, covered healthcare units that engage in patient care and electronic transactions related to eligibility and payment and non-covered healthcare units that do not transmit health information electronically in connection with a HIPAA-covered transaction but in some instances provide patient care and interact with protected health information for research, administrative, technical, or support purposes. These covered and non-covered healthcare units are collectively referred to as the “UCF Healthcare Component.” This policy also applies to business associates.

BACKGROUND INFORMATION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is about protecting patient information and giving patients control over the use and disclosure of their protected health information (PHI). HIPAA applies to specific types of entities and provides the minimum national standards for the protection of certain identifiable health information. UCF, as an academic institution, is not entirely bound by HIPAA but has HIPAA covered components and therefore is a Hybrid Entity under the regulation. This decision reflects its structure, which includes **Covered Healthcare Units** that provide patient care (subject to HIPAA if they electronically bill) and **Non-covered Healthcare Units** that do not transmit health information electronically in connection with a HIPAA-covered transaction but in some cases provide patient care and interact with protected health information for research, administrative, technical, or support purposes. Although these non-covered healthcare units are not directly subject to HIPAA, they must ensure proper handling and safeguarding of PHI in compliance with Florida law. Collectively, these units make up the UCF Healthcare Component. Identifiable health information pertaining to enrolled students is covered under the Family Educational Rights and

Protections Act (FERPA).

POLICY STATEMENT

The university is committed to protecting the privacy and security of patient information collected, maintained, used, and disclosed by the university and by those acting on its behalf, as permitted or required by law. The UCF Healthcare Component, and business associates where applicable, must comply with the requirements set forth in this policy and the corresponding HIPAA Privacy and Security Manual. Failure to comply with this policy or the HIPAA Privacy and Security Manual may result in disciplinary action, up to and including termination.

UCF personnel will not be considered in violation of university HIPAA policies, state law, or the HIPAA Privacy Rule when disclosing protected health information (PHI) as a whistleblower or as a victim of a crime, provided such disclosures meet applicable legal requirements see 45 CFR § 164.502(j) — Disclosures by whistleblowers and workforce member crime victims.

DEFINITIONS

Business Associate: Any person or organization outside a Covered Entity's Workforce with whom the Covered Entity shares Protected Health Information (PHI) to perform services. These services can include administrative tasks, billing, legal assistance, accreditation, consulting, storage, and other similar services. Before sharing PHI or UCF electronic PHI (ePHI) with a Business Associate, a Business Associate Agreement must be in place.

Covered Entity (Covered Healthcare Unit): A health plan, a health care clearinghouse, or a health care provider who transmits certain health information (including billing information) in electronic format. This includes any unit at UCF that provides medical or mental health services and electronically bills for those services.

Designated Record Set (DRS): Any grouping of information that includes PHI, and is gathered, stored, used, or shared by a Covered Entity to help make decisions about individuals. The Designated Record Set includes the following documents/files containing PHI:

a. Permanent clinical record
b. Billing record
c. Electronic record (e.g. Electronic Health Record, Practice Management System, Lab Information System, etc.)
d. Handheld devices

Hybrid Entity: HIPAA recognizes some entities perform both covered (health care services subject to billing) and non-covered (research, administrative, and support) functions and rather than requiring the whole entity to comply with HIPAA, such entity may claim a Hybrid Entity designation.

Individually Identifiable Health Information (per HIPAA): Health information that can be used to identify the individual it pertains to by examining identifiers. Specific identifiers include:

- Names
- Street address, city, county, precinct, or zip code
- Birth date, admission date, service date, discharge date, or date of death
- Age over 89
- Telephone numbers and fax numbers
- Email addresses
- Social security numbers
- Medical records numbers, health plan beneficiary numbers, account numbers
- Device identifiers and serial numbers
- Certificate/license numbers
- Vehicle identifier and serial number
- License plates
- URLs, IP addresses
- Full face photo
- Photo with distinctive tattoo

Protected Health Information (PHI): Individually Identifiable Health Information, associated with a health condition, provision of health care, or payment for health care, that is transmitted or maintained in any media or form (electronic, digital, video, audio, paper, or oral) by or on behalf of a Covered Entity. This includes the Designated Record Set and any other patient specific information used by UCF Personnel. For the purposes of this policy, PHI includes UCF Electronic Protected Health Information (ePHI).

UCF ePHI: ePHI generated by, or on behalf of, the UCF Health Care Component.

UCF Healthcare Component: UCF is a Hybrid Entity, consisting of both covered healthcare units that provide patient care (subject to HIPAA if they electronically bill) and non-covered healthcare units that do not transmit health information electronically in connection with a HIPAA-covered transaction but may still provide patient care and interact with PHI for research, administrative, technical, or support purposes. Collectively these units are known as the UCF Healthcare Component and subject to this policy and the HIAA Privacy and Security Manual. The UCF Healthcare Component is identified as follows:

Covered Healthcare Units

1. College of Health Professions and Sciences - Communication Disorders Clinic
2. College of Health Professions and Sciences - Physical Therapy Clinic
3. College of Medicine, including UCF Health, HealthARCH, Burnett School of Biomedical Sciences, and Health and Information Technology Department
4. UCF Health - Student Health Services, including UCF Pharmacy

Non-Covered Healthcare Units

1. Office of Research – Institutional Review Board (IRB)
2. College of Sciences – UCF RESTORES
3. Office of the General Counsel
4. Office of the General Counsel – Health Affairs Division
5. UCF Advancement Staff

6. UCF Department of Security
7. UCF Information Security Office (ISO)
8. UCF IT, Chief Technology Office:
   Telecommunications - Unified Communications, Network Services, Installation Maintenance Repair; Senior Director, Enterprise Infrastructure, Client Services - Support zones, Endpoint Engineering Services; Infrastructure – Tier 0/1, Cloud Services, Linux, and Data Centers
9. University Audit
10. Division of People and Workplace Experience (excluding Building Code Department)

UCF Personnel: Includes all employees, students, residents, fellows, and volunteers who are employed by, or acting on behalf of the UCF Healthcare Component.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity**.**

PROCEDURE

Using this policy and the corresponding HIPAA Privacy and Security Manual, the UCF Healthcare Components are expected to establish a process within their respective units addressing the following:

1. Reviewing and becoming familiar with this policy and the requirements in the HIPAA Privacy and Security Manual
2. Implementing the HIPAA Privacy and Security Manual and developing appropriate, unit-specific policies and procedures ensuring they are no less stringent than those contained in this policy and the HIPAA Privacy and Security Manual
3. Developing unit-specific operating procedures that delineate the steps to be performed to comply with the policies and procedures
4. Providing training on HIPAA requirements, policies, and procedures

The HIPAA Privacy and Security Manual will be reviewed annually and revised, to include new procedures, as needed when changes are made to applicable laws and/or university regulations or policies. Each UCF Healthcare Component shall include, in its processes, a mechanism for ensuring that corresponding updates to their unit-specific policies, procedures and operating procedures are completed.

RELATED RESOURCES

UCF HIPAA Privacy and Security Manual (insert link when posted)

HIPAA Resource

45 CFR 164

CONTACTS

Director, Privacy Compliance
HIPAA Privacy and Security
University Compliance and Ethics
4365 Andromeda Loop N., MH 396,
Orlando, FL 32816
privacy@ucf.edu

HIPAA Privacy and Security Manual

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and implementing regulations include the Privacy Rule, the Security Rule, and the Breach Notification Rule. The Privacy Rule applies to protected health information that is transmitted or maintained in any media or form – electronic, digital, video, audio, paper, or oral. The Security Rule deals specifically with protected health information held or transferred in electronic form. The Breach Notification Rule is triggered in an event of a privacy or security incident involving the compromise of protected health information. The University of Central Florida (UCF) is dedicated to ensuring full compliance with HIPAA.

HIPAA provides the minimum national standards for the protection of certain identifiable health information. State laws in some instances provide higher protections for sensitive medical information, such as mental health conditions and treatment, substance abuse and treatment, sexually transmitted diseases (STDs), tuberculosis (TB), Human Immunodeficiency Virus and Acquired Immunodeficiency syndrome (HIV)/AIDS, abortion, birth control, sickle cell anemia, and genetic diseases and genetic test results.

UCF, as an academic institution, is not entirely bound by HIPAA but has HIPAA covered components and therefore is a Hybrid Entity under the regulation. This decision reflects its structure, which includes **Covered Healthcare Units** that provide patient care (subject to HIPAA if they electronically bill) and **Non-Covered Healthcare Units** that do not transmit health information electronically in connection with a HIPAA-covered transaction but in some instances provide patient care and interact with protected health information (PHI) for research, administrative, technical, or support purposes. Although non-covered healthcare units are not directly subject to HIPAA, they must ensure proper handling and safeguarding of PHI in compliance with Florida law. Collectively, these two units (covered healthcare units and non-covered healthcare units) make up the UCF Healthcare Component and are identified as follows:

Covered Healthcare Units

1. College of Health Professions and Sciences - Communication Disorders Clinic
2. College of Health Professions and Sciences - Physical Therapy Clinic
3. College of Medicine, including UCF Health, HealthARCH, Burnett School of Biomedical Sciences, and Health and Information Technology Department
4. UCF Health - Student Health Services, including UCF Pharmacy

Non-Covered Healthcare Units

1. Office of Research – Institutional Review Board (IRB)
2. College of Sciences – UCF RESTORES
3. Office of the General Counsel
4. Office of the General Counsel – Health Affairs Division
5. UCF Advancement Staff

6. UCF Department of Security
7. UCF Information Security Office (ISO)
8. UCF IT, Chief Technology Office, Telecommunications - Unified Communications, Network Services, Installation Maintenance Repair; Client Services - Support zones, Endpoint Engineering Services; Infrastructure – Tier 0/1, Cloud Services, Linux, and Data Centers
9. University Audit
10. Division of People and Workplace Experience (excluding Building Code Department)

The university has oversight, compliance, and enforcement obligations. Unless otherwise specified, this HIPAA Privacy and Security Manual apply to the clinics, units, departments, faculty, and staff identified in the Health Care Component and Direct Support Organizations (DSO) as applicable.

Roles and Responsibilities

The University Privacy Officer with the office of Compliance and Ethics oversees the Privacy and Security manual, guides, monitors, and maintains the university's HIPAA privacy and security policies and procedures. The University Privacy Officer serves as the primary point of contact for all privacy-related matters, including receiving and addressing privacy complaints, inquiries, and concerns from faculty, staff, students, and the public. Additionally, the University Privacy Officer will ensure cooperation with regulatory agencies, including the U.S. Department of Health and Human Services' Office for Civil Rights.

Each **Covered Healthcare Unit** must designate and maintain a covered healthcare unit privacy officer or designee responsible for implementing this HIPAA Privacy and Security policy and procedure manual, developing and implementing unit-specific privacy policies, addressing privacy concerns, and keeping the University Privacy Officer informed of relevant updates. The covered healthcare unit privacy officer or designee must promptly report privacy complaints, suspected or confirmed breaches, and potential HIPAA violations to the University Privacy Officer. The covered healthcare unit Privacy Officer or designee is also responsible for conducting annual security risk assessments to support ongoing HIPAA compliance and must promptly inform the University Privacy Officer of any high-risk findings, material vulnerabilities, or significant compliance concerns identified through the assessment process.

TABLE OF CONTENTS

HIPAA Privacy and Security Sanctions Policy

DEFINITIONS

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA): The federal law that addresses the use and disclosure of individuals' protected health information by covered entities, establishes national standards for the protection of certain health information, and provides standards for individuals' privacy rights to understand and control how their health information is used.

2. Access: The ability or means necessary to make Electronic Health Information available for Exchange or Use.

3. Actor: A health care provider, health IT developer of certified health IT, health information network, or health information exchange (pertaining to Information Blocking).

4. Authorization: A signed, detailed document granting a healthcare provider permission to use or disclose an individual's Protected Health Information (PHI) for purposes other than treatment, payment, or healthcare operations.

5. Business Associate: Any person or organization outside a Covered Entity's Workforce with whom the Covered Entity shares Protected Health Information (PHI) to perform services. These services can include administrative tasks, billing, legal assistance, accreditation, consulting, storage, and other similar services. Before sharing PHI or UCF electronic PHI (ePHI) with a Business Associate, a Business Associate Agreement must be in place.

6. Covered Entity (Covered Healthcare Unit): A health plan, a health care clearinghouse, or a health care provider who transmits certain health information (including billing information) in electronic format. This includes any unit at UCF that provides medical or mental health services and electronically bills for those services.

7. Designated Record Set (DRS): Any grouping of information that includes PHI, and is gathered, stored, used, or shared by a Covered Entity to help make decisions about individuals. The Designated Record Set includes the following documents/files containing PHI:

a. Permanent clinical record
b. Billing record
c. Electronic record (e.g. Electronic Health Record, Practice Management System, Lab Information System, etc.)
d. Handheld devices

8. Disclosure: The release, transfer, provision of access to, or divulging of protected health information (PHI) outside the entity holding the information.

9. Electronic Health Information (EHI): Electronic protected health information contained in a Designated Record Set. It does not include psychotherapy notes or information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding. EHI also excludes any information that has been de-identified in accordance with HIPAA's de-identification standards.

10. Electronic Protected Health Information (ePHI): PHI in an electronic format.

11. Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

12. Exchange: The ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks.

13. Final HIPAA Omnibus Rule: The most recent HIPAA amendment implements several provisions of the HITECH Act, part of the American Recovery and Reinvestment Act of 2009, to enhance the privacy and security protections for health information established under HIPAA.

14. Health Information Technology for Economic and Clinical Health Act (HITECH Act): The federal law, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), amended HIPAA and addresses the privacy and security concerns associated with the electronic transmission of health information.

15. HIPAA Privacy Rule: The Rule that regulates the use and disclosure of all PHI including oral, paper, and electronic held by covered entities.

16. HIPAA Security Rule: The Rule that focuses specifically on ePHI. It establishes administrative, physical, and technical safeguards and identifies security standards for protecting certain health information that is held or transferred in electronic form.

17. Hybrid Entity: HIPAA recognizes some entities perform both covered (health care services subject to billing) and non-covered (research, administrative, and support) functions and rather than requiring the whole entity to comply with HIPAA, such entity may claim a Hybrid Entity designation.

18. Individually Identifiable Health Information (per HIPAA): Health information that can be used to identify the individual it pertains to by examining identifiers. Specific identifiers include:

- Names
- Street address, city, county, precinct, or zip code
- Birth date, admission date, service date, discharge date, or date of death
- Age over 89
- Telephone numbers and fax numbers
- E-mail addresses
- Social security numbers
- Medical records numbers, health plan beneficiary numbers, account numbers
- Device identifiers and serial numbers
- Certificate/license numbers
- Vehicle identifier and serial number
- License plates
- URLs, IP addresses
- Full face photo
- Photo with distinctive tattoo

19. Information Blocking: A practice that, except as required by law or covered by an exception set forth below, is likely to interfere with, prevent, or materially discourage Access, Exchange, or Use of EHI; and if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent or materially discourage Access, Exchange, or Use of EHI

20. Institutional Review Board (IRB): A committee that reviews and oversees research involving human subjects to ensure ethical standards are met and participants' rights and welfare are protected.

21. Minimum Necessary: Requires covered entities to restrict the use or disclosure of PHI to only the minimum amount needed to accomplish the intended purpose.

22. Non-Covered Healthcare Unit: Units at the university that provide patient care, even if not technically subject to HIPAA because they do not engage in electronic transactions related to eligibility and payment for care, and units that interact with PHI for research, administrative, technical, or support purposes.

23. Notice of Privacy Practices (NPP): A document that tells patients how a Covered Entity may use and disclose their PHI. The NPP also informs patients of their rights regarding PHI and includes information on how the patient can file a complaint. The content of the NPP is governed by HIPAA.

24. Part 2 Program: A *Part 2 Program* refers to any individual or entity that is federally assisted and provides substance use disorder (SUD) diagnosis, treatment, or referral for treatment, as defined in 42 CFR Part 2.

25. Personal Representative: A person authorized under applicable law to act on behalf of the patient in making healthcare-related decisions.

26. Personally Identifiable Information (PII): Personally Identifiable Information is referenced as “Personal Information” under Florida law, and means either of the following:

a. An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:
   i. A social security number;
   ii. A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
   iii. A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;
   iv. Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
   v. An individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term “Personal Information” does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term “Personal Information” also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

27. Protected Health Information (PHI): Individually Identifiable Health Information, associated with a health condition, provision of health care, or payment for health care, that is transmitted or maintained in any media or form (electronic, digital, video, audio, paper, or oral) by or on behalf of a Covered Entity. This includes the Designated Record Set and any other patient specific information used by UCF personnel. For the purposes of this manual, PHI includes UCF Electronic Protected Health Information (ePHI).

28. Sensitive Protected Health Information: PHI related to mental health conditions and treatment, sexually transmitted diseases, substance (drug and alcohol) abuse and treatment, genetic diseases and genetic test results, sickle cell anemia, tuberculosis, and HIV/AIDS (sensitive medical condition).

29. Strong Password: A password that is difficult to guess, consisting of eight (8) or more characters, including lower case and upper-case letters, numerals, and special characters. Longer passwords, or passphrases are, in general, more secure than shorter passwords.

30. UCF ePHI: ePHI generated by, or on behalf of, the UCF Health Care Component.

31. UCF Health Care Component: UCF is a Hybrid Entity, consisting of both covered healthcare units that provide patient care (subject to HIPAA if they electronically bill) and non-covered healthcare units that do not transmit health information electronically in connection with a HIPAA-covered transaction but may still provide patient care and interact with PHI for research, administrative, technical, or support purposes. Collectively these units are known as the UCF Healthcare Component.

32. UCF HIPAA Policies: A set of policies addressing HIPAA Privacy, HIPAA Security, and Florida patient confidentiality requirements. Other health care units at UCF (e.g., Counseling and Psychological Services) may voluntarily use the UCF HIPAA Policies as standards for protecting patient confidentiality.

33. UCF Personnel: Includes all employees, administrators, faculty, staff, students, residents, fellows, and volunteers who are employed by, or otherwise acting for or on behalf of the UCF Healthcare Component.

34. Use: The sharing, utilization, employment, or analysis of Protected Health Information (PHI) within an entity that maintains it.

35. Waiver (IRB): Is an exemption granted by an Institutional Review Board from certain regulatory requirements for research involving human subjects.

36. Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity.

DESIGNATION OF UNIVERSITY PRIVACY OFFICER

In accordance with federal regulation 45 CFR 164.530(a), the University of Central Florida has designated a University Privacy Officer responsible for overseeing the development, implementation, and enforcement of privacy policies and procedures in compliance with HIPAA and other applicable regulations.

The University Privacy Officer, under the direction of the Associate VP, Deputy Chief Compliance & Ethics Officer, shall develop, implement, and maintain the University's HIPAA policies and procedures.

The University Privacy Officer will serve as the primary point of contact for all privacy-related matters, including:

- Receiving and addressing privacy complaints, inquiries, and concerns from faculty, staff, students, and the public;
- Coordinating responses to potential or actual breaches of protected health information (PHI); and
- Ensuring cooperation with regulatory agencies, including the U.S. Department of Health and Human Services' Office for Civil Rights (OCR).

The University Privacy Officer will also ensure HIPAA related training, awareness, and monitoring efforts are implemented across the university.

PATIENT RIGHTS REGARDING PROTECTED HEALTH INFORMATION

Covered healthcare units must incorporate the following practices related to patient rights:

1. Right to a Notice of Privacy Practices
2. Right to Request Restrictions on Uses and Disclosures of Protected Health Information
3. Right to Request Confidential Communications
4. Right to Access Protected Health Information for Inspection and Copy
5. Right to Request Amendment of Protected Health Information
6. Right to an Accounting of Disclosures
7. Right to File a Complaint

1. Right to Notice of Privacy

Patients receiving care from UCF covered healthcare units have the right to the privacy of their Protected Health Information (PHI), as defined by HIPAA and applicable state laws, and in accordance with the guidance provided to the UCF Healthcare Component. Each new patient must receive a written Notice of Privacy Practices (NPP) on or before their first visit. The patient, or their authorized representative, will be asked to sign an acknowledgment confirming receipt of the NPP. The NPP must also inform patients that they may request an updated version if it is revised.

2. Right to Request Restrictions

Patients of covered healthcare units have the right to request restrictions on the use and disclosure of their PHI for treatment, payment, and health care operations. However, the covered healthcare unit does not have to agree to any requested restrictions, except in cases where restrictions are required by law (eCFR :: 45 CFR 164.522 -- Rights to request privacy protection for protected health information.). Upon request from a patient, the covered healthcare unit must agree to a restriction on the disclosure of PHI to a health plan if the disclosure pertains to payment or healthcare operations, is not required by law, and involves information related to a service or item that has been fully paid out-of-pocket by the patient or another party.

Patients do not have the right to request restrictions on the use and disclosure of PHI that are required by law, or for public health activities, mandatory abuse reporting, health oversight activities, judicial and administrative proceedings, law enforcement activities, coroner/medical examiner/funeral director duties, disclosures for organ transplant, or medical research (with certain restrictions), worker's compensation reporting, certain military and national security/intelligence activities, or disclosures to avert a serious threat to the safety or health of an individual.

Patients must submit requests for restrictions in writing to the covered healthcare unit (See: *HIPAA Privacy Request Form*). All requests must be reviewed by the covered healthcare unit privacy officer or designee to determine if they can comply with the patient's specific restriction request.

If the covered healthcare unit cannot comply, the patient will be notified in writing of such decision and rationale for denial.

If a covered healthcare unit agrees to the patient's request, the agreement must be documented in writing and must outline the unit's responsibility to follow the requested restrictions, except in

emergencies where using or disclosing the PHI is necessary for treatment. It is the patient's responsibility to notify other providers within and outside UCF regarding the restriction. The patient's restricted information must be flagged in the patient's medical record.

The covered healthcare unit will counsel patients on how a requested restriction may affect coordinated services delivered during the same visit and any related follow-up care.

In case of non-payment, the covered healthcare unit must make reasonable attempts to resolve payment issues with the patient prior to disclosing restricted patient information to a health plan.

Covered healthcare units may require payment in full at the time a restriction is requested to avoid non-payment issues.

Covered healthcare units may terminate the agreement if the patient agrees to or requests the termination in writing or orally.

Covered healthcare units may end the agreement by notifying the patient. The termination only applies to information created or received after the patient has been notified and does not affect any restrictions that are legally required.

A copy of all written documentation relating to requests for restrictions must be maintained in the patient's medical record and in a separate file by the covered healthcare unit privacy officer or designee for a minimum of six years from the date of the agreement.

Covered healthcare units must maintain an electronic log identifying their patients who have been granted restrictions and the type of restriction for reference when releasing PHI. (See: *Restriction Log*).

3. Right to Request Confidential Information by Alternate Means or in Alternate Locations

Patients have the right to request to receive confidential information by alternative means or in alternative locations.

Covered healthcare units must accommodate reasonable requests submitted in writing by the patient, who is not required to disclose the reason for the request (See: *HIPAA Privacy Request Form*).

All written requests to receive confidential information by alternate means or in alternate locations will be reviewed by the covered healthcare unit privacy officer or designee who will determine if the request can be granted.

All documents related to requests for confidential information must be maintained for a minimum of six years by the covered healthcare unit privacy officer or designee.

4. Right to Access, Inspect, and Obtain a Copy of Protected Health Information (PHI)

Patients have the right to access, inspect, and obtain a copy of their PHI maintained in the patient's medical record and/or billing record subject to certain exceptions.

All requests from a patient for access to inspect and/or copy their PHI must be submitted in writing to the covered healthcare unit privacy officer or designee as stated in the *Notice of Privacy Practices*.

Grant Access Request
If the patient's request is granted in whole or in part, the covered healthcare unit privacy officer or designee must:

(1) Inform the patient of the acceptance of the request;
(2) Respond to the request and arrange access within 30 days of the date the request was received;
(3) Provide access in a location agreeable to both parties; and
(4) Provide the patient with a copy in the form and format requested, if it is readily produceable; if not, provide a hard copy form or other form/format agreed to by the covered healthcare unit and the patient.

i. If the patient requests a copy of his/her medical record, the covered healthcare unit must provide a copy at a reasonable, fee-based cost per page of copy or labor costs related to electronic PHI and any cost to mail the information to the patient.
ii. If a covered healthcare unit is unable to take action on the request within 30 days after receiving the request, it may extend the time for response by up to 30 days, but must, within the original 30-day time frame, inform the patient in writing of the reasons for the delay and the expected date of access.
iii. The covered healthcare unit must arrange with the patient for a convenient time and place to inspect or obtain a copy of his/her medical record or mail the copy of the medical record at the patient's request.
iv. If the patient's request for access requests a copy of the medical record be sent to another person designated by the patient, the covered healthcare unit must provide a copy of the medical record to the designated person. The patient's request must be made via a signed Authorization or Release of Information (ROI) and clearly identify the designated person and where to send the copy of the medical record.
v. If a patient's medical information is maintained electronically, and the patient requests an electronic copy either for themselves or to be sent to a third party; the covered healthcare unit must provide it. This includes all relevant PHI in an electronically maintained designated record set (such as electronic health records or linked images/data), excluding psychotherapy notes and information prepared in anticipation of legal proceedings. The information must be provided at the time the request is fulfilled, in the electronic format requested by the patient, if it can be readily provided. If not, it must be provided in another readable electronic format agreed upon by both the patient and the covered healthcare unit.
vi. If the patient's medical information is maintained electronically and if the patient requests via signed Authorization or ROI, it must be emailed to the patient (or to a third party), the covered healthcare unit will respond to the individual as follows: "Transmission of PHI via email is an unsecured transmission that can result in the PHI being intercepted by a third party. If you still wish for your PHI to be emailed, please submit a written acknowledgment that you are aware of the risk of unauthorized access and further disclosure." Upon receipt of acknowledgement from the patient, the requested information can be sent via email.

Request Access Denial

A covered healthcare unit may deny a request within 30 days of receiving it for access in whole or in part without further review under the following circumstances:

(1) If, after review, it is determined that the information requested was obtained from someone other than a healthcare provider under a promise of confidentiality, and granting access to the information would likely reveal the source, the request can be denied;
(2) The requested records constitute psychotherapy notes;
(3) The information is being compiled in reasonable anticipation of use in civil, criminal, or administrative proceedings;
(4) Clinical Laboratory Improvement Amendment (CLIA) provisions prohibit access;
(5) The patient agreed to the denial of access as part of a research project;
(6) The PHI is subject to the federal Privacy Act Office of Privacy and Civil Liberties | Overview of The Privacy Act of 1974 (2020 Edition) and access would be denied under that law.
    i. If access is denied without the right of further review, the patient must be notified of the denial, the basis for the denial, and the process for making complaints.
    ii. If a patient is denied access to their health information but has the right to further review, they must be informed of their right to have the denial reviewed by a licensed healthcare professional. This reviewer is designated by the covered healthcare unit privacy officer or designee and must have had no involvement in the original denial decision. The covered healthcare unit privacy officer or designee will promptly forward the review request to the designated reviewer, who must decide within a reasonable timeframe whether to uphold or overturn the denial. If access is granted, the procedures outlined in *grant access approval* will be followed. If the denial is upheld, the patient must be notified in writing in a timely manner.
    iii. All written notices of denial must state the reason for the decision and inform the patient of their right to make a complaint to the Secretary of the Department of Health and Human Services (DHHS).

Copies of all documentation relating to requests for access must be maintained for a minimum of six years by the covered healthcare unit privacy officer or designee.

The documentation must include the designated record set and the titles of persons or offices responsible for receiving and processing requests for access.

5. Right to Request Amendment

Patients have the right to request amendment of their PHI during the time a provider maintains their medical record and/or billing record (See: *HIPAA Privacy Request Form*).

Covered healthcare units must review written requests that identify the PHI that is requested to be amended. Within 60 days of receipt of the request, the covered healthcare unit must respond and include a reason to either support or deny the request.

The covered healthcare unit will then proceed with making the amendment or denying the request (e.g., record is accurate and complete).

The covered healthcare unit privacy officer or designee will review all requests for amendment and will forward them to the medical provider on record to make the determination to accept or deny the request.

The covered healthcare unit may have a one-time extension of 30 days to comply with the request for amendment.

Within 60 days of the request the individual must be notified in writing of the delay, the reason for the delay, and when a response can be expected (no later than 90 days of the receipt of the request).

Request for Amendment Approval
If the request for amendment is accepted, the covered healthcare unit privacy officer or designee must oversee the process and ensure:

(1) PHI is amended within 60 days of the date of receipt of the request;
(2) The amendment is made to the appropriate medical and/or billing records;
(3) The patient is informed that the amendment has been made;
(4) Any individuals or entities identified by the patient as needing the amended information are notified;
(5) Any individuals, including Business Associates, or entities who have used or may use the patient's health information in a way that could harm the patient or affect their care, and whose information was changed, must be notified that amendments have been made;
(6) The amendment must be made by identifying the records in the designated record set that are affected by the amendment and adding or otherwise providing a link to the location of the amendment.

Request for Amendment Denial

The covered healthcare unit may deny the request for amendment if it determines that the PHI or record that is the subject of the request was:

(1) Not created by covered healthcare unit, unless the patient can provide a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
(2) Not part of the medical and/or billing record of the patient;
(3) Not available (e.g., psychotherapy notes or information compiled in anticipation of a legal proceeding); or
(4) The PHI is accurate and complete as it exists and does not require amendment.

If the request for amendment is denied, the covered healthcare unit privacy officer or designee will oversee the process and ensure a written denial is provided to the patient which includes:

(1) The basis for the denial;
(2) A statement that the patient has the right to submit a written statement of disagreement related to the denial and instructions as to how they can file such statement with the covered healthcare unit privacy officer or designee;
(3) A statement that informs the patient that they may request that the covered healthcare unit include the patient's request for an amendment and the denial, with any future disclosures of the PHI that is the subject of the amendment if a patient does not submit a statement of disagreement;
(4) A description of how the patient may make a complaint and who to submit it to (covered healthcare unit privacy officer or designee or to the Secretary of the Department of Health and Human Services).

(5) After receiving the statement, the covered healthcare unit Privacy Officer, or designee, in consultation with the University Privacy Office, will prepare a written rebuttal if one is warranted. A copy of the rebuttal must be provided to the patient and maintained in the patient's medical or billing record, as well as in a separate file.
(6) The covered healthcare unit must clearly identify the disputed information and link or attach the amendment request, the denial, the patient's statement of disagreement, and any rebuttal.

All documentation relating to requests for amendment must be maintained for a minimum of six years by the covered healthcare unit privacy officer or designee.

Covered healthcare units must make known the titles of persons or offices responsible for receiving and processing requests for amendment.

6. Right to an Accounting of Disclosures

Patients have the right to request a list (accounting) of disclosures of their medical or billing information made by the covered healthcare unit for purposes other than treatment, payment, or health care operations. This list must include disclosures made within the six years before the date of the request. Exempted from the accounting are the following disclosures:

(1) For purposes of treatment, payment, and health care operations
(2) To the individual
(3) To persons involved in the care of the individual
(4) For national security
(5) To correctional facilities and law enforcement officials
(6) Made pursuant to a valid authorization
(7) For purposes of a facility directory

Covered healthcare units must provide the patient with a written accounting no later than 60 days after receipt of the request:

(1) The written accounting of disclosures must include a list of all disclosures (except those exempted as noted above) made within six years of the date of the request, or a shorter period if requested by the patient. This includes any disclosures made to or by a Business Associate of the covered healthcare unit.
(2) The written accounting for each disclosure must include:
    i. The date of the disclosure;
    ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
    iii. A brief description of the PHI disclosed;
    iv. A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.
(3) If, during the period covered by the accounting, multiple disclosures of PHI have been made to the same person or entity for a single purpose, the accounting for disclosures must include:
    i. The information listed above for the first disclosure;
    ii. The frequency, periodicity, or number of the disclosures made during the accounting period; and
    iii. The date of the last disclosure during the accounting period.

If the covered healthcare unit is unable to provide the accounting within 60 days, it may extend the time period by no more than 30 additional days. This extension may be granted only once and must comply with the following conditions:

i. The covered healthcare unit must provide the patient with a written statement of the reasons for the delay including the date by which the accounting must be provided, within 60 days of the request.
ii. All documentation related to accounting disclosures must be maintained for a minimum of six years by the covered healthcare unit privacy officer or designee. The documentation must include the titles of persons or offices responsible for receiving and processing requests for an accounting of disclosures.

7. Right to File a Complaint

Patients have the right to file a complaint under HIPAA if they believe their privacy rights have been violated. Complaints can be submitted to the covered healthcare unit privacy officer or designee, the University Privacy Officer at privacy@ucf.edu, or to the U.S. Department of Health and Human Services at U.S. Department of Health & Human Services - Office for Civil Rights. Retaliation against any individual who files a complaint is strictly prohibited. Any suspected or reported retaliation must be promptly reported to the University Privacy Officer for review and handling.

ADDRESSING HIPAA PRIVACY COMPLAINTS

Covered healthcare units must provide an open, accessible, and non-retaliatory process for receiving, investigating, and resolving privacy related complaints involving PHI, for patients, their representatives, and UCF personnel. All complaints must be promptly reviewed, documented, and resolved in accordance with HIPAA regulations, UCF HIPAA policies, and applicable state law. Issues that rise to the level of a breach will be addressed under the separate Breach and Incident (Response and Reporting) Policies**.**

The covered healthcare unit privacy officer or designee is responsible for:

- Receiving and acknowledging complaints.
- Investigating complaints in a timely and thorough manner.
- Determining whether a HIPAA violation occurred and assessing its impact.
- Documenting findings, corrective actions, and communications.
- Ensuring no retaliation occurs against complainants.
- Coordinating with the University Privacy Officer and General Counsel as needed.

1. Submitting a Privacy Concern

Patients or their representatives: May submit complaints regarding HIPAA Privacy violations in accordance with the Notice of Privacy Practices**.**

UCF personnel: May submit complaints through their respective covered healthcare unit privacy officer or designee, University Privacy Officer (privacy@ucf.edu), to the UCF IntegrityLine (https://www.ucfintegrityline.com; 855-877-6049) or to the U.S. Department of Health and Human Services at U.S. Department of Health & Human Services - Office for Civil Rights.

2. Complaint Process

The covered healthcare unit privacy officer or designee must:

- Promptly notifying the University Privacy Officer of any complaints received.
- Acknowledge, review, log, and investigate all complaints.
- Determine whether a violation occurred, its impact, and the responsible party.
- Take steps to limit further unauthorized use or disclosure.
- Document findings and recommend corrective actions.
- Ensure appropriate steps are taken to prevent recurrence.

3. Documenting and Reporting

All violations, investigations, mitigation steps, and patient communications must be documented and retained for six years or as otherwise required by law.

The covered healthcare unit privacy officer or designee must notify the University Privacy Officer regarding:

- The nature of the violation.
- The impact on patient health or financial well-being.
- Workforce involvement and resulting sanctions, if applicable.
- Actions taken to mitigate harm.
- The effectiveness of mitigation activities and final disposition.

4. Non-Retaliation

Retaliation against any individual who files a complaint is strictly prohibited. Any suspected or reported retaliation must be promptly reported to the University Privacy Officer for review and handling.

NOTICE OF PRIVACY PRACTICES

Covered healthcare units must provide a Notice of Privacy Practices ("NPP") in accordance with the HIPAA Privacy Rule and applicable state laws, patients' rights, and legal duties of the covered healthcare units with respect to PHI. NPP describes uses and disclosures of PHI by a covered healthcare unit. The University Privacy Officer will provide a standard NPP outline with necessary HIPAA provisions for each covered healthcare unit. Each unit must customize the NPP to align with their operations, HIPAA, and Florida law, ensuring it addresses uses and disclosures that do not require patient authorization. The University Privacy Officer must review and approve covered healthcare units Notice of Privacy Practices prior to posting.

1. Each covered healthcare unit must provide an NPP to all patients by the date of their first service, including any electronic services. The NPP must also be posted in a visible and accessible location where patients can easily read it. Patients may request a paper copy of the NPP during their visit to the unit.
2. Covered healthcare units with websites offering information about customer services or benefits must prominently display the NPP on the site and provide electronic access to it.
3. If the first service is delivered electronically, the covered healthcare unit must automatically provide an electronic NPP at the time of the patient's initial request for service.
4. Covered healthcare units must make a good faith effort to obtain a return receipt or other transmission indicating receipt of NPP.
5. The patient or their Personal Representative can request a paper copy of the NPP from the covered healthcare unit at any time.
6. Covered healthcare units can send the NPP by email if the patient agrees to receive it electronically and hasn't withdrawn their consent. If the email transmission fails, a paper copy must be provided.

Content of the Notice of Privacy Practices

1. Header of the NPP - The following statement must appear as a header or otherwise be prominently displayed:

"THIS NPP DESCRIBES HOW MEDICAL/HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

2. <u>Uses and Disclosures</u>

The NPP must be written in plain language and contain:

i. A clear explanation to inform the individual about uses and disclosures and at least one example the covered healthcare unit is permitted to make for each of the following purposes: treatment, payment, and health care operations.

ii. A description of the uses and disclosures of PHI that require Authorization (See: *Uses and Disclosures of Protected Health Information when Patient Authorization is Required*).

iii. A statement that other uses and disclosures not described in the NPP will be made only with the individual's written Authorization, and that the individual may revoke the Authorization in writing except to the extent that the covered healthcare unit has already acted based on it.

iv. A description of uses and disclosures of PHI not requiring consent or authorization.

v. A specific statement from the covered healthcare unit that maintains psychotherapy notes, explaining that most uses and disclosures of those notes require written authorization.

vi. A statement that uses and disclosures of PHI for marketing purposes require an Authorization (and specific consent under Florida law).

vii. A statement that any sale of PHI requires an Authorization.

viii. A statement that PHI may be used or disclosed for fundraising purposes, but the patient has a right to opt-out of receiving such communication (with each solicitation). Also, a statement that specific consent under Florida law or Authorization may be required when a covered healthcare unit intends to contact a patient to raise funds for its operations.

ix. The date on which the NPP is first in effect, which may not be earlier than the date on which the NPP is printed or otherwise published.

x. Contact information for additional questions about the covered healthcare unit's privacy policies.

3. Individual Rights

The NPP must contain a statement of the patient's rights with respect to PHI and a brief description of how the patient may exercise these rights. (Refer to: *Patient's Rights Regarding Protected Health Information)*.

4. Acknowledgement

Except in an emergency treatment situation, covered healthcare units must make a good faith effort to obtain a written acknowledgement of receipt of the NPP from new patients or document their good faith efforts to obtain such acknowledgement and the reason why the acknowledgement was not obtained.

5. Legal Duties and Privacy Practices of Covered Healthcare Unit

i. A statement that the covered healthcare unit will maintain the privacy of PHI.

ii. A statement that the covered healthcare unit will notify affected patients (or their legal representatives) following a breach of unsecured PHI.

iii. A statement that the covered healthcare unit will abide by the terms of the NPP currently in effect.

iv. A statement that the covered healthcare unit can update its NPP, and any changes will apply to all PHI it holds.

v. A statement that the covered healthcare unit will provide patients with a revised NPP upon request, as well as have it posted in a clear and prominent location and have copies available at the facility.

vi. A statement that patients may contact the covered healthcare unit (including contact information and the process) or the U.S. Department of Health and Human Services for Civil Rights at 200 Independence Avenue, S.W., Washington, D. C. 20201, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/ with a complaint if the patient believes their privacy rights have been violated, and that the patient will not be retaliated against for filing a complaint.

6. Required NPP Elements for Part 2 Programs

Covered healthcare units must include the following statements in their NPP when they maintain or use Substance Use Disorder (SUD) records:

Uses and Disclosures of SUD Records

I. A statement that SUD records may be used and disclosed for treatment, payment, and healthcare operations only when a valid Part 2–compliant Authorization (or single patient consent) has been completed.

II. A statement that SUD records received from another Part 2 program remain protected under 42 CFR Part 2 and may only be used or disclosed as allowed by the patient's Authorization.

III. A statement explaining that, without authorization, SUD records may be disclosed only in limited circumstances permitted by law (e.g., medical emergencies, court order, research, audit/evaluation).

IV. A statement that any party receiving SUD records from the covered healthcare unit is prohibited from redisclosing that information unless expressly permitted by 42 CFR Part 2.

V. A statement that SUD records are protected by federal confidentiality laws, including 42 CFR Part 2, which provide stronger protections than HIPAA for these records.

VI. A statement that SUD information cannot be used or disclosed in civil, criminal, administrative, or legislative proceedings without the patient's written authorization or a specific court order that provides the patient notice.

VII. A statement that all SUD records will include the required Part 2 confidentiality notice when disclosed to others.

7. NPP Revisions

The covered healthcare unit must promptly revise and distribute its NPP whenever there is a material change to its legal duties, the uses or disclosures of PHI, patient's rights, or other privacy practices in the NPP.

8. Document Retention

Covered healthcare units must keep copies of their NPPs and any signed acknowledgments or records of efforts to get an acknowledgment for six years from the date the NPP was last in effect.

Sample Notice of Privacy Practices

AUTHORITY

45 CFR § 164.520

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

(MINIMUM NECESSARY REQUIREMENTS)

Covered healthcare units must use, share, and request PHI only as allowed by HIPAA, the HITECH Act, the HIPAA Omnibus Rule, and applicable Florida law. All uses, disclosures, and requests will be limited to the minimum necessary, unless broader sharing is legally permitted.

Covered healthcare units must receive Authorization from the patient or their representative prior to any use or disclosure of PHI, except where otherwise permitted under HIPAA, Florida law, or UCF HIPAA Policies. The Authorization must meet all applicable legal requirements for content and execution.

In cases where covered healthcare units are permitted to use or disclose PHI without patient authorization, or when patients must be given the opportunity to agree or object, UCF personnel must follow the appropriate procedures to ensure compliance with legal and policy standards.

Covered healthcare units must make a good faith effort to obtain the patient's written acknowledgement of receipt of the Notice of Privacy Practice and any necessary consents under Florida law. Covered healthcare units must use and disclose PHI only as necessary to carry out treatment, payment, or health care operations and obtain the patient's authorization for use or disclosure of PHI where required by HIPAA.

UCF personnel must receive relevant training based on their job responsibilities regarding:

a. Definitions of treatment, payment, and health care operations;

b. Use and disclosure of PHI for treatment, payment, and health care operations;

c. When an Authorization is needed for use or disclosure of PHI;

d. When the patient has the right to an opportunity to agree or object to use or disclosure of PHI and related procedures;

e. When PHI can be used or disclosed without Authorization or the opportunity to agree or object;

f. When and how to track and account for disclosures; and

g. Additional rules on requirements regarding confidentiality as imposed by federal and state law.

1. Minimum Necessary Requirements

a. Covered healthcare units must identify uses of PHI for treatment, payment, health care operations, research, administrative, technical, or support purposes and will use only the minimum amount of information that is reasonably necessary to achieve the purpose for the use of PHI.

b. Covered healthcare units must implement this policy (as appropriate) addressing access to, and use of, PHI by personnel based on the individual's specific job duties.

c. Covered healthcare units must implement UCF HIPAA policies and procedures that limit the disclosure or request for PHI, on a routine and recurring basis, to the amount reasonably necessary to achieve the purpose of the use and/or disclosure. Note that the minimum necessary requirement does not apply to disclosure or requests of PHI for treatment purposes.

d. For all disclosures and requests for PHI that are not routine, covered healthcare units must:

i. Develop unit specific policies and procedures to limit the PHI disclosed to that information which is reasonably necessary to accomplish the purpose for which the disclosure is sought; and

ii. Review requests for disclosure on an individual basis in accordance with the established criteria.

e. Covered healthcare units may rely on a requester's representation that the information sought reflects the minimum necessary amount of PHI when the request originates from one of the following:

i. A public official, if they confirm that the information is the minimum needed for the stated purpose(s),

ii. Another appropriate HIPAA covered entity,

iii. A professional who is part of the Workforce or a Business Associate of the covered healthcare unit, providing services to the unit, if they confirm that the information is the minimum necessary for the stated purpose (s), or

iv. A person requesting the information for research purposes, provided they submit the required documentation. (See: *Uses and Disclosure of Protected Health Information for Research*).

v. Covered healthcare units can rely on a representation that the PHI requested is the minimum necessary for research when the researcher provides the following:

a. An IRB approval letter

b. Review of PHI is required to prepare a research plan or for other similar activities before conducting research

c. Review of decedent PHI is necessary for research

f. Covered healthcare units must not disclose, use, or request an entire medical record, except when the entire record is specifically justified as needed to accomplish the purpose for the use, disclosure, or request.

2. **Exceptions to Minimum Necessary Requirements** - The minimum necessary requirement applies to all uses, disclosures, and requests of PHI apart from the following:

a. Disclosures or requests to a health care provider for treatment
b. Requests by a health care provider for treatment
c. Uses or disclosures made to the patient, or when an individual requests access to their own medical or billing information, or when made in accordance with the rights to request access and an accounting of disclosures
d. Uses and disclosures made based on an Authorization
e. Disclosures made to the Secretary of DHHS for HIPAA enforcement
f. Uses or disclosures required by law, limited to what the law requires
g. Uses and disclosures that are required for compliance with HIPAA laws and regulations

3. Disclosures for Health Oversight Activities - Covered healthcare units may disclose PHI to health oversight agencies for activities authorized by law. Activities may include, but are not limited to, state licensing inspections, reimbursement audits, and other regulatory reviews.

4. Disclosures by Whistleblowers and Personnel Crime Victims – UCF personnel will not be in violation of UCF HIPAA policies if they disclose PHI as a whistleblower or a victim of a crime 45 CFR § 164.502(j) — Disclosures by whistleblowers and workforce member crime victims.

A. 1. The disclosure of PHI by a whistleblower is not a violation of UCF HIPAA Policies, state law, or HIPAA Privacy Rule if the individual believes in good faith that:

a. The covered or non-covered healthcare unit has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or

b. The care, services, or conditions provided by the covered or non-covered healthcare unit potentially endangers one or more patients, workers, or the public.

2. To qualify as a whistleblower, the disclosure of PHI must be to a:

a. Health oversight agency

b. Public health authority

c. Health care accreditation organization

d. Attorney retained by or on behalf of the individual to determine his/her legal options pertaining to the observed conduct

B. 1. The disclosure of PHI to a law enforcement official by UCF personnel who is a victim of a crime is not considered a violation of UCF HIPAA Policies, state law, or the HIPAA Privacy Rule if:

a. The PHI disclosed is about the suspected perpetrator of the criminal act; and

b. The PHI disclosed is limited to:

i. Name and address
ii. Date and place of birth
iii. Social security number
iv. ABO blood type and rh factor
v. Type of injury
vi. Date and time of treatment
vii. Date and time of death, if applicable
viii. Description of distinguishing physical characteristics including:
(1) Height
(2) Weight
(3) Gender
(4) Race
(5) Hair and eye color
(6) Presence or absence of facial hair
(7) Scars
(8) Tattoos

5. **Documentation and Record Retention Requirements** - Covered healthcare units must document disclosures using the PHI disclosure log and must retain any related documentation for a minimum of six years.

6. Non-Covered Healthcare Units (HIPAA Aligned UCF Requirements)

Non-covered healthcare units are not subject to HIPAA requirements however they must ensure proper handling and safeguarding of PHI in compliance with Florida law. To promote consistent privacy protections across the UCF Healthcare Component, non-covered healthcare units are expected to:

Limit uses and disclosures of PHI to what is reasonably necessary to accomplish the purpose of the request or activity.

1. Access or share only the minimum amount of identifiable health information needed to perform assigned duties.
2. Use or disclose PHI only for legitimate university operational purposes, and refrain from unnecessary or unrelated sharing.
3. Avoid using PHI for purposes inconsistent with the reason it was collected, unless required by law or approved by the appropriate UCF authority.
4. Document or record only the minimum necessary PHI when creating notes, files, or communications needed for operational purposes.
5. Ensure staff are trained on standards for appropriate uses, disclosures, and minimum necessary requirements when handling PHI.

AUTHORITY

45 CFR § 164.502(b) and § 164.514(d)