Policy Title: Creation and Use of De-Identified Health Information for Educational Purposes

1.0 Purpose

To comply with certain provisions of the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act (HITECH), and the associated regulations (collectively known as "HIPAA") regarding the creation and use of de-identified health information.

2.0 Policy Statement

Clinical education and training activities of learners is an essential mission to UCF COM. Similarly, UCF COM considers HIPAA compliance and respect of patient privacy of utmost importance. All learners are expected to be knowledgeable about UCF COM HIPAA policies and related procedures. This policy sets out the methodology of appropriately de-identifying health information for use in the educational setting. Only the de-identified health information shall be used or disclosed for educational purposes.

De-identified health information is not considered PHI (see definition below) and is not subject to the restrictions on uses and disclosures set forth in HIPAA. UCF COM learners, faculty (core, volunteer, affiliate) and staff may use PHI to create de-identified health information for educational purpose by using the Safe Harbor Method under the HIPAA Privacy Rule.

3.0 Definitions

De-identified health information: Health information that does not identify an individual and with respect to which ***there is no reasonable basis to believe that the information can be used to identify an individual***. As per US Department of Health and Human Services, PHI may be de-identified by using either of the following methods: The Safe Harbor Method, or Expert Determination Method.

Protected Health Information (PHI): Any type of Individually Identifiable Health Information, whether electronically maintained, electronically transmitted, or in any other format or medium (i.e., discussed orally, on paper or other media, photographed or otherwise duplicated). PHI includes all medical, dental, social, demographic, laboratories, imaging, billing, and any other patient related data or information.

4.0 Methodology

For purposes of this policy, the selected methodology for de-identifying health information for use in the educational setting is the Safe Harbor Method**.**

Learners, faculty (core, volunteer, affiliate) will use the Safe Harbor Method for de-identifying protected health information, and de-identified health information shall not be re-identified.

Per the Safe Harbor Method, PHI is considered de-identified if all of the following identifiers of the individual or the individual's relatives, employers, or household members are removed:

1. Name
2. Address - all geographic subdivisions smaller than a state - including street address, city, county, precinct, zip code, and their equivalent geocodes.
3. All elements of dates (except year) for dates directly related to birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers (bank, retirement, credit card, etc.)
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plates
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers including fingerprints and voice prints
17. Full face photographic images or comparable images; and
18. Any other unique identifying number, characteristic or code. For purposes of this policy, a unique identifying characteristic includes:
    a) Patient's initials (first, last or combination of both initials)
    b) Name/Location (including city) of hospital or clinic
    c) Name of Preceptor or Provider that the patient is seeing in the clinical setting
    d) Place or name of organization of Employment for the patient

AND

The information could not be used alone or in combination with other information to identify an individual who is the subject of the information.

5.0 Monitoring/Procedures:

Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with rules and/or policies of UCF COM and UCF.

6.0 Key Search Words:

HIPAA	Privacy and Security	Formative feedback

7.0 Revision History

Version	Date Approved	Modifications
V1	6/21/2024	Original

6.0 References:

US Department of Health and Human Services:https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard)

45 CFR 164.308(a)(3)(ii)(c)

45 CFR 164.530(c)(1)

UCF Regulations Chapter UCF-3

HIPAA Privacy and Security Sanctions Policy