ADMINISTRATIVE REQUIREMENTS OF HIPAA

Policy: The University of Connecticut will comply with all administrative requirements of the Health Insurance Portability and Accountability Act.

Rationale: To maintain compliance with Title 45 CFR Part 164.530, Administrative Requirements.

I. General Procedures:

1. The University has assigned the role of University's HIPAA Privacy Officer to the Assistant Director of Compliance in the Office of Audit, Compliance & Ethics to serve as a privacy official who is responsible for the overall guidance, monitoring and maintenance of the privacy policies and procedures for University.

2. The University has assigned the role of University's HIPAA Security Officer to the Chief Information Security Officer (CISO) in UITS to serve as a security official that is responsible for overall guidance, monitoring and maintenance of the security policies and procedures for the University.

3. Each of the University's HIPAA-Covered Components shall designate and maintain a contact person who will serve as an internal privacy contact ("privacy liaison") for the individual unit, who is responsible for receiving complaints and who is able to provide further information about matters covered by the Notice of Privacy Practices (the "NPP").

4. Each of the University's HIPAA-Covered Components shall designate and maintain a contact person or office who will serve as an internal data security contact ("security liaison") for the individual unit, who is responsible for monitoring and/or overseeing the Component's compliance with the HIPAA Security Rule and for reporting compliance related security incidents and/or breaches to the University's Security Officer.

5. Each of the HIPAA-Covered Components of the University will make the University's HIPAA Privacy and Security policies and procedures available through a Notice of Privacy Practices (NPP). The NPP shall be provided to clients/patients (hereinafter "Individuals") as follows:

    - The NPP will be distributed and/or made available to directly to Individuals receiving services from the HIPAA-covered component,
    - A copy of the NPP will be posted in the main reception area of the unit, and
    - A link to the NPP will be located on the HIPAA-covered component's web page.

Training:

6. The University will train all persons covered by the requirements set forth in this *Manual* on all relevant policies and procedures that have been implemented to protect and secure PHI. The training will be customized as appropriate for the different roles filled by faculty, staff, students, and volunteers as well as affiliates of the HIPAA-covered component (hereinafter "members") who may have access to PHI.

7. The University will provide training that meets the following requirements:
    a. To each new member of the HIPAA-Covered Component within a reasonable period of time after the person joins the Component;
    b. To each member of the HIPAA-Covered Component who has changed job functions and is impacted differently by the privacy policies and procedures;
    c. To each member of the HIPAA-Covered Component whose functions are affected by a change in the HIPAA regulations; and
    d. To each member of the HIPAA-Covered Component whose functions are affected by a material change in the policies or procedures.

8. The University will also provide refresher training to all members on an annual basis.

9. The HIPAA-Covered Component will document that the training has been provided, in either written or electronic format, and retain the documentation for a minimum of six (6) years.

Safeguards:

10. The University will have in place appropriate administrative, technical, and physical safeguards to protect the privacy and ensure the data security of PHI.

11. The University will reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of HIPAA.

Complaints:

12. Each HIPAA-Covered Component will provide a process for Individuals to make complaints concerning the University's policies and procedures or its compliance with such policies and procedures.

13. As part of the process, each HIPAA-Covered Component shall ensure that all complaints and suspected and/or actual security incidents are reported to the University's Privacy Officer and Security Officer.

14. The HIPAA-covered Component will document all complaints received, and their disposition, if any, in written or electronic form. These documents must be retained for a minimum of six (6) years.

Sanctions:

15. If members of its workforce fail to comply with the privacy policies and procedures of the University or the requirements of HIPAA, the HIPAA-Covered Component and/or the University will use the disciplinary procedures currently defined at the University to apply appropriate sanctions.

16. Any member of the HIPAA-Covered Component that becomes aware of a violation or deviation from the University's Privacy policies and procedures should notify the HIPAA-covered component's privacy liaison as soon as possible.

17. Any member of the HIPAA-Covered Component that becomes aware of a security incident, an actual or potential breach or a violation or deviation from the University's Security policies and procedures should notify the HIPAA-Covered Component's security liaison as soon as possible.

18. Sanctions may include, but are not limited to:
    a. Counseling
    b. Oral Warning
    c. Written Warning
    d. Suspension
    e. Termination

19. Disciplinary sanctions and appeals are handled in accordance with applicable procedures, depending on the type of workforce member being disciplined, for example:
    a. If the individual accused of the violation belongs to a collective bargaining union, involvement by the Office of Faculty & Staff Labor Relations (OFSLR) and union representation may be necessary to protect the rights of the member
    b. If the person accused of the breach is a faculty member, the process will be as outlined under applicable by-laws

20. Reporting a violation in bad faith or for malicious reasons may be interpreted as a misuse of the reporting mechanism(s) and may result in disciplinary action.

21. As outlined in Part 164.502(j) of the HIPAA Privacy regulations, a disclosure that is made by a member of the HIPAA-Covered Component's workforce is not subject to sanction if the disclosure is part of a "whistleblower" action. To meet this condition, the disclosure must be made to a health oversight agency or public health authority authorized to investigate HIPAA privacy violations or to an

attorney retained to determine the legal options of the person making the disclosure.

22. If the HIPAA-Covered Component becomes aware of a use or disclosure of PHI that violates its privacy policies and procedures, the HIPAA-Covered Component shall work to mitigate, to the extent practicable, any harmful effect of the violation.

Refraining From Intimidating or Retaliatory Acts:

23. The University will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
    a. Any Individual for the exercise of any right under, or for participation in any process established by the Health Insurance Portability and Accountability Act, including the filing of a complaint;
    b. Any Individual for:
        i. Filing of a complaint with the Secretary under subpart C of part 160 of Title 45 of the Code of Federal Regulations;
        ii. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
        iii. Opposing any act or practice believed to be unlawful, provided the person has a good faith belief that the practice is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information.

Waiver of Rights:

24. The University will not require Individuals to waive their rights to make a complaint to the Secretary of Department of Health and Human Services. The University will also not require Individuals to waive their rights to make a complaint as a condition of the provision of treatment, payment, or eligibility for benefits.

Policies and Procedures

25. The University's policies and procedures are designed to comply with the standards, implementation specifications or other requirements of the Health Insurance Portability and Accountability Act of 1996. Applicable policies and procedures are reasonably designed to ensure compliance, taking into account the types of activities related PHI that are performed by the University's HIPAA-Covered Components.

Changes to Policies or Procedures.

26. The University will change its policies and procedures as necessary and appropriate to respond to changes that may be made to the standards,

requirements, and implementation specifications of the Health Insurance Portability and Accountability Act of 1996.

27. When the University changes a privacy or data security practice that is described in the Notice of Privacy Practices (NPP) and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the NPP revision.

28. When the University changes a privacy or data security practice that is described in the NPP and makes corresponding changes to its policies and procedures, it will provide a copy of the revised NPP to Individuals on their next visit to the HIPAA-Covered Component. The revised NPP will be posted in the University's HIPAA-Covered Component units and available through the HIPAA-Covered Component's web pages.

Documentation:

29. The University shall:
    - Maintain its HIPAA privacy and security policies and procedures in written or electronic form;
    - Maintain a written or an electronic copy as documentation if a communication, action, activity, or designation is required to be in writing; and
    - Retain the documentation for a minimum of six (6) years from the date of its creation or the date when it last was in effect, whichever is later.