

**Interim Health Insurance Portability and Accountability Act Policy (Senate Document #18-19-05)****TO Wallace D. Loh | President****FROM Christopher Walsh | Chair, University Senate**

I am pleased to forward the accompanying legislation for your consideration and approval. Chair Walsh presented the revisions to the Interim Health Insurance Portability and Accountability Act Policy (Senate Document #18-19-05), which the University Senate reviewed as an informational item at its meeting on November 7, 2018. Please inform the Senate of your decision and any administrative action related to your conclusion.

Approved:

A handwritten signature in black ink, appearing to read "Wallace D. Loh", written over a horizontal red line.

**Wallace D. Loh
President****Date:****11-27-2018**

Copies of this approval and the accompanying legislation will be forwarded to:

Mary Ann Rankin, Senior Vice President and Provost
Reka Montfort, Executive Secretary and Director, University Senate
Michael Poterala, Vice President and General Counsel
Cynthia Hale, Associate Vice President for Finance and Personnel
John Bertot, Associate Provost for Faculty Affairs
Elizabeth Beise, Associate Provost for Academic Planning & Programs
Sylvia B. Andrews, Academic Affairs
Warren Kelley, Assistant Vice President for Student Affairs
David McBride, Director, University Health Center



Interim University Of Maryland Policy On Compliance With The Health Insurance Portability And Accountability Act

PRESENTED BY Christopher Walsh, Chair

REVIEW DATES SEC – September 21, 2018 | SENATE – November 7, 2018

VOTING METHOD For information only

RELEVANT POLICY/DOCUMENT [VI-24.00\(A\) University of Maryland Policy on Compliance with the Health Insurance Portability and Accountability Act](#)

NECESSARY APPROVALS N/A

ISSUE

In order to ensure continued compliance with Department of Health and Human Services regulations, the University established a small working group led by the UMD HIPAA Privacy Officer to review the University of Maryland Policy on Compliance with the Health Insurance Portability and Accountability Act. The working group consulted with the Office of General Counsel, the Division of Information Technology's Chief Information Security Officer, and the HIPAA Privacy Officer in the Health Center to make non-substantive revisions to the policy to ensure compliance. These revisions primarily involve updating names, internal operational procedures, and the list of units in Attachment A.

RECOMMENDATION(S)

The interim University of Maryland Policy on Compliance with the Health Insurance Portability and Accountability Act should be codified as policy once the University Senate is informed of the revisions.

COMMITTEE WORK

The Senate Executive Committee (SEC) reviewed the proposed revisions to the policy at its September 21, 2018 meeting and agreed that the changes did not warrant review by a Senate committee, as they are non-substantive in nature. However, in order to maintain an accurate historical record of the revisions and to ensure that members of the campus community are made aware of the revisions, the SEC voted to place the policy and associated revisions on the November 7, 2018 Senate meeting agenda as an informational item.

ALTERNATIVES

The original policy could remain unchanged. If the policy is not revised to align with federal regulations, the University could be fined for not being in compliance with the Department of Health and Human Services.

RISKS

There are no known risks to the University to accepting these revisions.

FINANCIAL IMPLICATIONS

There are no known financial implications.

VI-24.00(A) UNIVERSITY OF MARYLAND POLICY ON COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
(Approved by the President, March 20, 2003; amended on an interim basis by the President, July 18, 2018 pending University Senate Review)

I. GENERAL

The policy of the University of Maryland, College Park is to comply with the Health Insurance Portability and Accountability Act of 1996¹ and its implementing regulations² (collectively “HIPAA”) to the extent that HIPAA is applicable to the University.

II. STATUS AS HYBRID ENTITY

The University’s activities include both HIPAA covered and non-covered functions. Accordingly, the University has determined that it is a hybrid entity for HIPAA coverage purposes.

III. DESIGNATIONS

The University has designated its Health Care Component, as set forth in Attachment A to this policy. A unit is included in the designation only to the extent it performs HIPAA covered functions or engages in activities that would make it a business associate of a unit that performs covered functions if the two were separate legal entities (“~~eCovered~~ ~~u~~Unit”). Other units that perform health care functions **not covered by HIPAA, may and that (1)** voluntarily choose to comply with or participate in some or all HIPAA requirements, policies or procedures; **or (2) desire to become a Covered Unit must first receive approval from the University. A unit must be included in Attachment A before engaging in HIPAA covered activities.** ~~Such voluntary compliance or participation shall not affect a unit’s status as a non-covered component.~~

The University has designated a Privacy Officer for HIPAA compliance purposes. The HIPAA Privacy Officer designation and contact information are posted on the University’s HIPAA Website <http://hipaa.umd.edu>.³ The designation of the Privacy Officer is subject to change by the President.

The Privacy Officer is responsible for the development and implementation of policies and procedures as required by HIPAA, **in consultation with the Office of ~~Legal~~ General Counsel.** The Privacy Officer may amend the University’s designation of ~~eCovered~~ ~~u~~Unit(s) from time to time, as appropriate. The Privacy Officer is also designated to receive complaints concerning the University’s HIPAA related policies and procedures and HIPAA compliance. ~~and to provide further information about matters covered by the~~ **Any unit that engages in a HIPAA covered function must have a University’s Notice(s) of Privacy Practices.**

¹ 42 U.S.C. 1320d, *et seq.*

² CFR Parts 160, 162, 164.

³ The name and contact information for the Privacy Officer may also be obtained from the Office of the ~~Senior Vice President for Academic Affairs and Provost at 301-405-5252~~ **Vice President for Student Affairs at 301-314-8436** or via email at HIPAA-Privacy@umd.edu.

Each eCovered uUnit shall designate a Privacy Coordinator to interact with the Privacy Officer and coordinate HIPAA compliance within the unit. Documentation of each Privacy Coordinator designation shall be provided to and maintained by the Privacy Officer.

IV. IMPLEMENTING POLICIES AND PROCEDURES

The University's Privacy Officer is responsible for adopting and implementing general operating policies governing HIPAA compliance by the Health Care Component. Such policies shall be distributed to all eCovered uUnits and posted on the University's HIPAA Website.

Each eCovered uUnit is responsible for complying with the HIPAA operating policies, as applicable, and for developing procedures and forms as needed to implement and comply with such policies and HIPAA, including appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. Each eCovered uUnit is also responsible for providing the University's Privacy Officer with current copies of its procedures and any forms or other HIPAA related documents. The Privacy Officer may require a eCovered uUnit to change its procedures, forms, or related documents.

V. HIPAA ADVISORY COMMITTEE

The University has established a HIPAA Advisory Committee to assist the Privacy Officer and oversee the University's HIPAA compliance. The Privacy Officer shall chair the committee. One member of the committee shall be designated by each of the following offices: Senior Vice President ~~for Academic Affairs~~ and Provost, Vice President and Chief Information Officer, **Vice President and General Counsel, Vice President for Student Affairs**, Vice President for Research, and Dean of the Graduate School. The University's **Chief Information Technology** Security Officer will also serve on the committee. Additional members may be appointed by the Privacy Officer. ~~The Office of Legal Affairs will provide advice to the committee.~~

VI. COMPLAINTS

Complaints concerning the University's HIPAA policies and procedures and/or compliance with those policies and procedures or HIPAA shall be made in writing to the Privacy Officer. The Privacy Officer shall investigate all complaints in a timely manner and provide a written determination to the parties involved (e.g., the complainant and the eCovered uUnit(s).) The Privacy Officer shall document all complaints received and their disposition.

VII. NO RETALIATION

Neither the University, nor any of its employees, will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for exercising of any rights under, or participating in any process established by, the HIPAA privacy regulations, including filing a complaint; or

2. Any person for:
 - a. filing a complaint with the U.S. Secretary of Health and Human Services (or any other officer or employee of HHS to whom the authority has been designated) under the HIPAA regulations;
 - b. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
 - c. opposing any act or practice made unlawful by the HIPAA privacy regulations, provided the person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy regulations.

VIII. TRAINING

The University will train members of its workforce (faculty, staff, students, and volunteers) in each eCovered uUnit on policies and procedures with respect to protected health information as required by HIPAA. Such training will be as necessary and appropriate for the members of the workforce to carry out their function within the eCovered uUnit. The Privacy Officer, in conjunction with the Office of General Counsel and the units' Privacy Coordinators, ~~is responsible for developing training materials and implementing and overseeing workforce training~~ will define requirements regarding workforce training.

~~Training shall be provided not later than April 13, 2003. Thereafter, e~~Each new member of a eCovered uUnit's workforce shall be trained within a reasonable time after joining the workforce. Additional training will be provided to each member of a eCovered uUnit's workforce whose functions are materially affected by a change in HIPAA related policies or procedures. Such training will be provided within a reasonable time after the material change becomes effective.

The Privacy Officer, and the Privacy Coordinators for the Covered Units ~~designated components~~, shall maintain copies of the training materials and document that the required training has been provided.

IX. WAIVER OF RIGHTS

Individuals will not be required to waive their rights to file a complaint under the HIPAA privacy regulations as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

X. MITIGATION

The University will mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure, by the University or its business associates, of protected health information in violation of its policies and procedures or the HIPAA privacy regulations.

XI. SANCTIONS

Violation of this policy by a member of the University's workforce is subject to appropriate personnel or other disciplinary action.

XII. DOCUMENTATION

All policies, procedures, communications, actions, activities and/or designations that require documentation under HIPAA shall be maintained in written and/or electronic form and retained for a period not less than six years from the date of its creation or the date when it was last in effect, whichever is later.

The University's Privacy Officer will determine whether documentation required by HIPAA and/or this policy should be kept centrally by the Privacy Officer, or whether any eCovered uUnit will be responsible for keeping its own documentation as required by HIPAA. The Privacy Officer has the authority to require any eCovered uUnit to send all documentation to him/her.

XIII. AMENDMENT

The University may change this policy and any other the policies or procedures described herein as necessary and appropriate, in accordance with standard University procedures and any applicable HIPAA requirements.

Attachment A
Designated Health Care Component

| <u>Health Care Provider Unit(s)</u> | <u>When Added</u> |
|--|---------------------------|
| University Health Center | April 14, 2003 |
| | |
| <u>Business Associate Type Units</u> (To the extent that person unit engages in covered activities) | <u>When Added</u> |
| Chief Information Security Officer, Division of Information Technology | April 14, 2003 |
| Office of General Counsel Legal Affairs | April 14, 2003 |
| HIPAA Privacy Officer , Office of VP for Student Affairs; HIPAA Privacy Officer Designated Individuals | September 3, 2009 |
| Bursar's Office | April 14, 2003 |
| Including individuals not within the office who have access to billing records | |
| | |
| Office Division of Information Technology, Subunits | |
| User Support Services | April 14, 2003 |
| Network Operations | April 14, 2003 |
| LAN Services | April 14, 2003 |
| Applications Development | April 14, 2003 |