

University of Maryland Baltimore (UMB) Information Technology Privacy Policy

Effective Date: 04/14/03

Purpose

To establish a framework for the privacy of sensitive information which is accessible through the use of UMB information technology resources.

Definitions

"FERPA": Family Educational Rights and Privacy Act, sometimes referred to as the Buckley Amendment, a federal law that gives students certain rights concerning their educational records kept by UMB.

"Gramm-Leach-Bliley Act (GLB Act)": a federal law that applies to UMB when it is involved in awarding certain student loans.

"HIPAA": Health Insurance Portability and Accountability Act of 1996, a federal law.

"Information technology resources" or "IT Resources": information technology resources including, but not limited to, computerized information, computing facilities, systems and devices, network systems, resources and devices, software, e-mail systems, and web pages.

"IT Administrator": the administrator or academic officer of a UMB unit or school who, as determined by the applicable vice president or dean, is responsible for management and oversight of the UMB IT Resources and Affiliate IT Resources located in, or used by Personnel of, that unit or school.

"Maryland Law": those provisions of the Annotated Code of Maryland which pertain to the confidentiality of personal information about employees, students, research subjects, clients or patients of UMB.

"Sensitive information": Personal, medical, confidential and otherwise legally protected information which is maintained in, or available through use of, UMB IT Resources.

"UMB": University of Maryland Baltimore.

General Policy

The University of Maryland Baltimore (UMB) recognizes and respects the need for privacy of sensitive information. Maintaining the security of sensitive information is one of the University's most important responsibilities. UMB's IT administrators or their authorized representatives are held accountable for adhering to strict standards to prevent the misuse of sensitive information. Sensitive information is safeguarded in the following ways:

1. Employee access to sensitive information is restricted to individuals on a "need to know" basis for the sole purpose of conducting the business of the University.
2. UMB emphasizes the importance of confidentiality and privacy through a combination of training, operating procedures, and systematically enforced information technology security.
3. UMB strictly adheres to FERPA, HIPAA, GLB, Maryland Law, and other relevant federal and state laws to protect the security of sensitive information.
4. UMB continually tests and updates our information technology resources to improve the protection of sensitive information residing on University servers.

At times, UMB is legally required to disclose sensitive information, e.g., in response to a valid subpoena or to comply with a legally permitted inquiry by a governmental agency or regulatory body. UMB may exchange some sensitive information with other entities in order to carry out normal University business transactions. Legal requirements concerning use and disclosure of sensitive information will be applied to information maintained with IT Resources to the same extent that the requirements are applied to records in other forms.

For detailed information, refer to other pertinent documents such as the UMB Information Technology Acceptable Use Policy, the UMB Information Technology Security Policy, the UMB Policy on the Privacy of Protected Health Information, as well as UMB policies of general application relating to FERPA and HIPAA.

APPROVED BY THE PRESIDENT:

David J. Ramsay, D.M., D.Phil.

Date