
 POLICIES	HIPAA/HITECH	Page 1 of 7
	Effective Date: 09/23/2009	
Retired:	Revised: July 1, 2011	
Approved by: WAYNE J. RILEY, M.D., MPH, MBA, PRESIDENT AND CEO 		
Subject: Office of Corporate Compliance - Breaches of Unsecured Protected Health Information		

SCOPE: This policy applies to Meharry Medical College (MMC), its participating physicians and clinicians, and all College employees and business associates, contractors, sub-contractors, who provide management, administrative, financial, legal and operational support to or on behalf of MMC.

PURPOSE: To provide for notification in the case of breaches of unsecured protected health information. For purposes of these requirements, set forth in section 13402(h) of the HITECH Act ("Act").

POLICY STATEMENT: MMC is required by law to protect the privacy of health information that may reveal the identity of a patient. If a breach of certain types of individually identifiable health information occurs, MMC is required to provide notification to certain individuals and entities pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), which is Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) and any regulations promulgated there under.

Therefore, MMC, will implement reasonable and appropriate technologies and methodologies designed to secure protected health information from unauthorized disclosure.

MMC may also have additional reporting obligations under other federal laws and state breach notification laws. Those obligations are not addressed in this policy.

DEFINITIONS: The term "**breach**" means the acquisition, access, use or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information.

The term "**protected health information**" (PHI) means any patient information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

The term "**unsecured protected health information**" means PHI that is not

Subject: Breaches of Unsecured Protected Health Information

secured through the use of approved technologies or methodologies.

The term “**approved, technologies and methodologies**” means that it must render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

DISCOVERY OF BREACH

Breaches are treated as discovered as of the first day on which the breach is known or should have been known to MMC (or business associate). Once a breach is discovered the Privacy Officer must notify patients without unreasonable delay but not later than 60 calendar days after discovery. If the breach requires the involvement of law enforcement, the notification may be delayed for a period of time as determined by a law enforcement official.

A breach is treated as discovered when College

- has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach; or
- is deemed to have knowledge of the breach because a workforce member or agent of the College has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach.

BREACH REPORTING

It is the responsibility of the College to protect and preserve the confidentiality of all PHI. To avoid possible breaches of PHI and inform the members of MMC and business associates of the importance of promptly reporting privacy and security incidents and the consequences for the failure to do so.

Any member or business associate of MMC who knows, believes, or suspects that a breach of PHI has occurred, must report the breach to his or her supervisor or the Privacy Officer immediately. Please do not fear retaliation if you report a breach. Breaches may also be reported anonymously via Compliance Hotline (888) 695-1534 or compliance@mmc.edu.

After a potential breach is reported, the Privacy Officer will work with the HIPAA Information Security Officer and the information technology department to conduct a thorough investigation, which includes an analysis to determine whether a breach of unsecured PHI under HITECH has occurred and if so, what notifications are required. The Privacy Officer should complete its investigation generally within [20] calendar days to ensure sufficient time for the preparation and coordination of notifications, if required, provided that the investigation may take more or less time depending on the circumstances. As part of the investigation, the Privacy Officer will take all necessary steps to mitigate any known harm.