MEHARRY MEDICAL COLLEGE **POLICIES**	**HIPAA/HITECH**	**Page 1 of 7**
	Effective Date: September 23, 2009	
Interim Date: July 21, 2015	**Revised: July 1, 2015**	
Approved by: James E. K. Hildreth, Ph.D., M.D. **President and Chief Executive Officer**		
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

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.

If the information is not PHI because, for example, the information is de-identified in compliance with HIPAA, or does not include certain identifiers as set forth in HIPAA, no further investigation is required under HITECH. The Privacy Officer will have other responsibilities, including evaluating whether notifications are required pursuant to the Red Flag Rules and/or applicable state breach notification laws.

If the information is PHI, the Privacy Officer will then need to determine if the information has been properly "secured" by the methods set forth in HITECH (e.g. encryption and destruction). If the Privacy Officer determines that the PHI is "secured," although no further steps are required pursuant to this policy, the Privacy Officer is responsible for determining whether the MMC has accounting and mitigation obligations under HIPAA. If it is determined that the PHI is unsecured, the Privacy Officer must determine whether a breach under HITECH has occurred.

METHODS OF PROTECTION

Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.

a. Encryption – MMC and each business associate will implement and maintain reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.

b. Destruction – MMC and each business associate will implement destruction techniques that render PHI unusable and/or unreadable in any format.

PHI secured by one of the above methods is not unsecure and is therefore not subject to this policy.

NOTIFICATION OF BREACH

In the event a breach of unsecured PHI is discovered, the Privacy Officer is required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed, according to the requirements of the Act:

- Written notice to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual);

- In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period

determined by HHS) on the home page of the web site of the College or notice in major print or broadcast media and must include a toll-free number;

- In cases that the College deem urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.

The Privacy Officer must prepare a notification that includes (to the extent possible):

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the MMC is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site or postal address.

If the breach affects 500 or more patients, then a notice must also be provided to major media outlets. Additionally, The Privacy Officer must notify HHS Secretary immediately. The HHS website will have a list that identifies all of the covered entities involved in a breach in which more than 500 individual are affected.

The Privacy Officer will be sensitive to only include general information (i.e. listing the types of information involved as opposed to listing the actual PHI that was involved in the breach) in the notification. Depending upon the nature of the breach and the information obtained during the investigation, the Privacy Officer may also include:

- Recommendations that the individual contact applicable credit card companies and information about how to obtain credit monitoring services;
- Information about the steps the College is taking to retrieve the breached

information and improve security to prevent future breaches; and

- Information about sanctions the MMC imposed on its workforce members involved in the breach.

To comply with other applicable laws, the Privacy Officer may also need to translate the notice into other languages and make the notice available in alternate formats, such as Braille, large print or audio.

DETERMINATION OF BREACH

If the Privacy Officer has determined that there is an acquisition, access, use or disclosure of unsecured PHI, the Privacy Officer must then conduct the following analysis:

1. Determine whether there has been an impermissible acquisition, access, use, or disclosure of PHI under the HIPAA Privacy Rule.

2. If no, no further analysis required pursuant to this policy. If yes, determine whether the impermissible acquisition, access, use, or disclosure compromises the security or privacy of the PHI.

3. If no, no further analysis required pursuant to this policy. If yes, determine whether an exception applies.

Impermissible Acquisition, Access, Use, or Disclosure

PHI may only be used or disclosed pursuant to a valid authorization or one of the specifically enumerated exceptions under HIPAA. To determine if PHI was impermissibly acquired, accessed, used or disclosed under the HIPAA Privacy Rule, the Privacy Officer will conduct an analysis. If the acquisition, access, use, or disclosure is permitted, no further investigation pursuant to this policy is required. If the Privacy Officer determines that an impermissible acquisition, access, use, or disclosure has occurred, he/she is responsible for complying with the applicable policies and procedures (including making an accounting of such disclosure and, if necessary, mitigating any known harm) and conducting the analysis set forth below.

Compromises the Security or Privacy of PHI

If there has been an impermissible acquisition, access, use, or disclosure of unsecured PHI under the HIPAA Privacy Rule, the Privacy Officer must then perform a risk assessment to determine if there is a significant risk of financial, reputational or other harm to the individual whose PHI was used or disclosed.

If the information increases the risk of identity theft (i.e. SSN, account number or

mother's maiden name). The Privacy Officer should carefully conduct a fact intensive investigation that includes any type of health information that may cause reputational harm.

If the Privacy Officer determines that there is no significant risk of harm to the individual, no further steps need to be taken pursuant to this policy. The Privacy Officer, however, is responsible for conducting a separate analysis regarding the College's accounting and mitigation obligations, if any.

Exceptions to the Definition of Breach

If, based on the above analysis, the Privacy Officer determines that there has been an impermissible acquisition, access, use, or disclosure which compromises the security or privacy of the PHI, the Privacy Officer must determine if any of the following exceptions apply:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the College or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;
- Any inadvertent disclosure by a person authorized to access PHI at the College or business associate to another person authorized to access PHI at MMC or business associate, or organized health care arrangement in which the College participates, and the information received from such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or
- Disclosure of PHI where the College or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

TRACKING

The College shall maintain a breach notification log and submit report required annually to the Secretary of HHS documenting the breaches that have occurred and have been discussed, prepared and finalized for submission to the Secretary on or before March 1.

SANCTIONS: Any member of the College who violates this policy will be subject to disciplinary action up to and including termination of employment with Meharry Medical College. Anyone who knows or has reason to believe that another person

has violated this policy should report the matter promptly to his or her supervisor or the College's Privacy Officer. All reported matters will be investigated and, where appropriate, steps will be taken to remedy the situation. Where possible the College will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment with Meharry Medical College.

EXHIBITS: