

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 1 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

Tulane University Policy: Response to Breach of Unsecured Protected Health Information

SCOPE OF POLICY

This policy applies to Tulane University Medical Group, its participating physicians and clinicians, and all University employees and business units who provide management, administrative, financial, legal and operational support to or on behalf of Tulane University Medical Group and have been designated as part of the Tulane University HIPAA Health Care Component (Health Care Component).

STATEMENT OF POLICY

The Health Care Component 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, the Health Care Component 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, which is Title XIII of the American Recovery and Reinvestment Act of 2009 and any regulations promulgated thereunder (HITECH). The Health Care Component may have additional reporting obligations under other federal laws and state breach notification laws. Those obligations are not addressed in this policy.

IMPLEMENTATION OF POLICY

A. Definition of Breach

For the purposes of the policy, 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” 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.

B. Report of Breaches to Privacy Official

It is the responsibility of the Health Care Component to protect and preserve the confidentiality of all protected health information. To avoid possible breaches of protected health information and inform the members of the Health Care Component of the importance of promptly reporting privacy and security incidents and the consequences for the failure to do so, the Privacy Official will coordinate with other officials and departments to train all members of the Health Care Component on their respective responsibilities and obligations under HIPAA and HITECH, which will include a review of the protective procedures outlined in *GC-009-Confidentiality of Protected Health Information*. In addition to training the members of the Health Care Component, the Privacy Official may re-evaluate persons authorized to access protected health information to determine if authorization is necessary and, if necessary, whether such access complies with the minimum necessary standard under HIPAA.

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 2 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

Any member of the Health Care Component who knows, believes, or suspects that a breach of protected health information has occurred, must report the breach to the Privacy Official or the Office of the General Counsel immediately. Within one business day of its receipt of a report, the Privacy Official will notify the Office of the General Counsel (or vice versa).

After a potential breach is reported, the Privacy Official will work with other officials and departments, including the Office of the General Counsel and, if necessary, 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 protected health information under HITECH has occurred and if so, what notifications are required. The Privacy Official 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 Official will take all necessary steps to mitigate any known harm. The details of the investigation will be documented in a memo that is kept on file with the Privacy Official with a copy sent to the Office of the General Counsel.

As part of the Privacy Official's investigation to determine whether a breach of unsecured protected health information under HITECH has occurred, the Privacy Official must take certain steps to ensure a complete investigation. Exhibit I attached hereto provides an general overview of the more detailed process outlined below.

The Privacy Official must first decide whether the information is protected health information and if so, whether the protected health information is unsecured.

- *If the information is not protected health information* 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 Official 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 protected health information*, the Privacy Official 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 Official determines that the protected health information is "secured," although no further steps are required pursuant to this policy, the Privacy Official is responsible for determining whether the Health Care Component has accounting and mitigation obligations under HIPAA. If it is determined that the protected health information is unsecured, the Privacy Official must determine whether a breach under HITECH has occurred (see Part C).

The Privacy Official must document the analysis performed to determine if the information is protected health information, and if, necessary, whether the protected health information is secured, in a memo to be kept on file with the Privacy Official with a copy to be sent to the Office of the General Counsel.

As discussed in more detail in Part D below, if a breach under HITECH has occurred and notifications are required, the time period by which notifications must be sent to the affected individuals, the Secretary, and if, necessary, the media begins when the breach is first discovered, not when the Privacy Official completes its investigation of whether a breach has occurred. A breach is treated as discovered when the Health Care Component

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 3 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

(i) has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach; or

(ii) is deemed to have knowledge of the breach because a workforce member or agent of the Health Care Component has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach.

The Privacy Official will document when the Privacy Official reasonably believes the breach occurred.

C. Determination of Breach

If the Privacy Official has determined that there is an acquisition, access, use or disclosure of unsecured protected health information, the Privacy Official must then conduct the following analysis:

1. Determine whether there has been an impermissible acquisition, access, use, or disclosure of protected health information 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 protected health information.
3. If no, no further analysis required pursuant to this policy. If yes, determine whether an exception applies.

1. Impermissible Acquisition, Access, Use, or Disclosure

Protected health information may only be used or disclosed pursuant to a valid authorization or one of the specifically enumerated exceptions under HIPAA (See GC-009-*Confidentiality of Protected Health Information*). To determine if protected health information was impermissibly acquired, accessed, used or disclosed under the HIPAA Privacy Rule, the Privacy Official will conduct an analysis (the results of which will be detailed in a memo that is kept on file with the Privacy Official with a copy sent to the Office of the General Counsel). If the acquisition, access, use, or disclosure is permitted, no further investigation pursuant to this policy is required. If the Privacy Official 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 in #2 below.

2. Compromises the Security or Privacy of Protected Health Information

If there has been an impermissible acquisition, access, use, or disclosure of unsecured protected health information under the HIPAA Privacy Rule, the Privacy Official must then perform a risk assessment to determine if there is a significant risk of financial, reputational or other harm to the individual whose protected health information was used or disclosed. The Privacy Official will consider a number of factors, including:

- Who impermissibly disclosed or to whom the information was impermissibly disclosed (i.e. was the acquisition, access, use, or disclosure to a covered entity or business associate, or to a private individual or entity). There may be less risk of harm to the individual if the recipient of the information is obligated by HIPAA and HITECH.
- The likelihood the information is accessible and usable by the unauthorized individual.

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 4 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

- Whether the Health Care Component has taken immediate steps to mitigate, including obtaining assurances from the recipient that the information will not be further used or disclosed, or that the information is destroyed or returned prior to it being improperly accessed.
- The type and amount of protected health information involved. The Privacy Official must examine the information that was acquired, accessed, used or disclosed, including whether the information involved the name of the individual and that services were received, the types of services received or where the services were received (i.e. at a specialized facility or department) and if the information increases the risk of identity theft (i.e. SSN, account number or mother's maiden name). The Privacy Official should carefully conduct a fact intensive investigation that includes any type of health information that may cause reputational harm.

The Privacy Official will document the risk assessment in a memo that is kept on file with the Privacy Official with a copy sent to the Office of the General Counsel. If the Privacy Official 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 Official, however, is responsible for conducting a separate analysis regarding the Health Care Component's accounting and mitigation obligations, if any.

3. Exceptions to the Definition of Breach

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

- Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity 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 protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity 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 protected health information where a covered entity 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.

The Privacy Official will perform a fact specific analysis to determine if an exception applies and document its analysis and findings in a memo that is kept on file with the Privacy Official with a copy sent to the Office of the General Counsel. If an exception applies, the Privacy Official can conclude that a breach did not occur and that no notification is required.

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 5 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

If none of these exceptions apply, the Privacy Official must conclude that a breach of unsecured protected health information has occurred and notification to affected individuals, the Secretary of HHS (Secretary) and, if applicable, the media is required.

D. Breach Notification

Once the Privacy Official has determined that a breach has occurred, he/she is responsible for coordination of a response to certain persons and entities.

Notification to Affected Individuals

Notification must be provided to each individual whose unsecured protected health information has been or is reasonably believed to have been, acquired, accessed, used or disclosed as a result of the breach without unreasonable delay and in no case later than 60 calendar days. 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.

The Privacy Official 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 protected health information 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 Health Care Component 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.

The Privacy Official will be sensitive to only include general information (i.e. listing the types of information involved as opposed to listing the actual protected health information 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 Official 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 Health Care Component is taking to retrieve the breached information and improve security to prevent future breaches; and
- Information about sanctions the Health Care Component imposed on its workforce members involved in the breach.

To comply with other applicable laws, the Privacy Official 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.

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 6 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

The Privacy Official will send a draft of the notice to the Office of the General Counsel and the Office of Public Affairs for review. The preparation and review of the notice should be completed within [15] calendar days (more or less time may be necessary depending on the circumstances).

The notice will be sent by first-class mail or, if the Health Care Component does not have sufficient contact information for some or all of the affected individuals, by substitute notice (depending on the number of individuals for whom the Health Care Component does not have sufficient contact information, through an alternate form of written notice, by telephone or other means, or by a posting on [list web site] for 90 days or in major print or broadcast media in geographic areas where the affected individuals likely reside).

Notification to the Secretary

The Privacy Official must provide notice to the Secretary concurrently with the notification sent to the affected individuals (for any breach involving 500 or more individuals) or within 60 days after the end of each calendar year (for breaches involving less than 500 individuals). In the latter case, the Privacy Official will maintain a log and other documentation of each breach to ensure that the scope and extent of the information provided to the Secretary is in compliance with HITECH. The content of the notice will be the same as described above.

No later than November 30 of each year, the Privacy Official and the Information Security Officer will meet to discuss the process and content of the report to be sent to the Secretary. The Privacy Official and Information Security Officer will prepare a draft of the report and by January 31, will send the draft to the Office of the General Counsel. By February 15, the Office of the General Counsel, the Privacy Official and the Information Security Officer will finalize the report for submission to the Secretary on or before March 1.

Notification to the Media

The Privacy Official may also be required to notify a prominent media outlet for any breach that involves more than 500 residents of any one state or jurisdiction. The notification will contain the same information as described above and will be made concurrently with the notification sent to the affected individuals. The Privacy Official, depending on the circumstances of the breach, will determine what constitutes a prominent media outlet.

The Privacy Official will be responsible for documenting that all notifications required under HITECH were made in a memo to be kept on file with the Privacy Official with a copy to be sent to the Office of the General Counsel.

Notification by Business Associates

The Office of the General Counsel will work with business associates of the Health Care Component to ensure that business associates report any breaches of protected health information promptly to the appropriate individual at the Health Care Component.

To the extent the unsecured protected health information is the protected health information of a covered entity that participates in an organized health care arrangement with the Health Care Component, the Privacy Official will coordinate with the respective Privacy Official(s) of such covered entities.

VIOLATIONS

The Privacy Official has a general responsibility for implementation of this policy. Any member of the Health Care Component who violates this policy will be subject to disciplinary action up to and including termination of

Tulane University

DEPARTMENT: General Counsel's Office – HIPAA/HITECH	POLICY DESCRIPTION: Response to Breach of Unsecured Protected Health Information
PAGE: 7 of 7	
APPROVED: 9/23/09	REVISED:
EFFECTIVE DATE: 9/23/09	POLICY NUMBER: GC-026

employment with Tulane University. 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 University's Privacy Official. All reported matters will be investigated and, where appropriate, steps will be taken to remedy the situation (See Attachment – *Minimum Privacy Violation Action*). Where possible the University 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 Tulane University.

QUESTIONS

If you have questions about this policy, please contact the Privacy Official immediately.