

Tulane University

DEPARTMENT: General Counsel's Office -- HIPAA	POLICY DESCRIPTION: Confidentiality of Protected Health Information
PAGE: 1 of 4	
APPROVED: April 1, 2003	REVISED: July 1, 2005
EFFECTIVE DATE: April 14, 2003	POLICY NUMBER: GC-009

Tulane University Policy: Confidentiality of 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.

STATEMENT OF POLICY

The Tulane University Health Care Component is committed to protecting the privacy and confidentiality of health information about its patients. Protected health information is strictly confidential and should never be given, nor confirmed to anyone who is not authorized under the Tulane University Health Care Component policies or applicable law to receive this information.

IMPLEMENTATION OF POLICY

A. Definition of Protected Health Information

For purposes of the policy, 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.

This policy applies to protected health information in any form including spoken, written, or electronic form. It is the responsibility of the Tulane University Health Care Component to protect the privacy and preserve the confidentiality of all protected health information. This includes, but is not limited to, compliance with the protective procedures below.

B. Public Viewing/Hearing

The staff of the Tulane University Health Care Component is expected to keep protected health information out of public viewing and hearing. For example, protected health information should not be left in conference rooms, out on desks, or on counters or other areas where the information may be accessible to the public or to other employees or individuals who do not have a need to know the protected health information. Medical staff and support staff should also refrain from discussing protected health information in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients. Medical staff and support staff should also take care in sharing protected health information with families and friends of patients. Such information may generally only be shared with a personal representative, a family member, relative, or close personal friend who is involved with the patient's care or payment for that care. Even in the latter circumstance, information cannot be disclosed unless the patient has had an opportunity to agree or object to the disclosure, and staff may only disclose information that is relevant to the involvement of that family member, relative, or close personal friend in the patient's care or payment for the patient's care, as the case may be.

Tulane University

DEPARTMENT: General Counsel's Office -- HIPAA	POLICY DESCRIPTION: Confidentiality of Protected Health Information
PAGE: 2 of 4	
APPROVED: April 1, 2003	REVISED: July 1, 2005
EFFECTIVE DATE: April 14, 2003	POLICY NUMBER: GC-009

C. Databases and Workstations

The staff of the Tulane University Health Care Component is expected to ensure that they exit any confidential database upon leaving their workstations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. They are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any password, personal identification number, token or access card, or electronic signature. Each employee of the Tulane University Health Care Component is responsible for all activity occurring under his or her account, password, and/or electronic signature. These activities may be monitored.

D. Downloading, Copying, or Removing

The staff of the Tulane University Health Care Component should not download, copy, or remove from the clinical areas any protected health information except as necessary to perform their duties. Upon termination of employment with the Tulane University Health Care Component, or upon termination of authorization to access protected health information, the employees must return to the University any and all copies of protected health information in their possession or under their control.

E. Emailing and Faxing Information

The staff of the Tulane University Health Care Component should not transmit protected health information over the Internet (including e-mail) and other unsecured networks unless it has been encrypted and password protected, and the Security Officer approves the process used. Transmission of protected health information is permitted by fax using the following guidelines:

1. Always include a cover sheet with the faxed information and confidentiality statement:

© Confidentiality Notice

The documents accompanying this transmission contain confidential privileged information. The information is the property of the sender and intended only for use by the individual or entity named above. The recipient of this information is prohibited from disclosing the contents of the information to another party.

If you are neither the intended recipient or the employee or agent responsible for delivery to the intended recipient, you are hereby notified that disclosure of contents in any manner is strictly prohibited. **Please notify [name of sender] at [facility name] by calling [phone #] immediately if you received this information in error.**

2. Limit manual faxing to urgent transmittals:
 - A. Faxing PHI is appropriate only when the information is needed immediately for patient care.
 - B. Medical emergencies (*e.g.* ER or emergency surgery).
 - C. Other situations considered urgent (*e.g.* results from lab to physicians).

Tulane University

DEPARTMENT: General Counsel's Office -- HIPAA	POLICY DESCRIPTION: Confidentiality of Protected Health Information
PAGE: 3 of 4	
APPROVED: April 1, 2003	REVISED: July 1, 2005
EFFECTIVE DATE: April 14, 2003	POLICY NUMBER: GC-009

3. Unless necessary to treat in emergency situations, highly sensitive or personal information should be strictly limited when faxing. In general, this information should not be faxed:

- A. Drug dependency
- B. Alcohol dependency
- C. Mental illness or Psychiatric information
- D. Sexually transmitted disease (STD) information
- E. HIV status
- F. Genetic test results

Note: The policy on *Sensitive Information*, GC-023, contains additional information about protections for highly sensitive information under Louisiana law.

4. There are times when faxing highly sensitive information would be appropriate:

Example: Faxing PHI to a hospital's emergency room regarding the HIV status of a pregnant patient in labor.

5. Location of the Fax Machine:

- A. Should be secure whenever possible.
- B. Make sure that area is not accessible to the public.
- C. When possible, locate the machine in an area that requires security keys or badges for entry.

6. Mitigation of faxes sent to the incorrect party or sent in error:

- A. Practice should make reasonable efforts to obtain the copies from the recipient and see that they are destroyed.
- B. If copies cannot be retrieved due to number of copies and cost to return, and the fax recipient is a known business associate, verbal documentation of the destruction of the information is sufficient.
- C. If the information is inadvertently sent to a patient-restricted party or to a recipient where there is a risk of release of the PHI (e.g. newspaper), the Privacy Official should be notified and legal counsel should become involved for further instructions.

Tulane University

DEPARTMENT: General Counsel's Office -- HIPAA	POLICY DESCRIPTION: Confidentiality of Protected Health Information
PAGE: 4 of 4	
APPROVED: April 1, 2003	REVISED: July 1, 2005
EFFECTIVE DATE: April 14, 2003	POLICY NUMBER: GC-009

VIOLATIONS

The Privacy Official has a general responsibility for implementation of this policy. The staff of the Tulane University Health Care Component who violate this policy will be subject to disciplinary action up to and including termination of 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 your department supervisor or the Privacy Official immediately.

Minimum Privacy Violation Action

Level and Definition of Violation	Example of Violation	Action
<ul style="list-style-type: none"> • Accidental and/or due to lack of proper education. 	<ul style="list-style-type: none"> • Improper disposal of PHI. • Improper protection of medical records or other PHI. <ul style="list-style-type: none"> ▪ Leaving records on counters or where otherwise accessible by unauthorized individuals. ▪ Leaving any documents that contain PHI in inappropriate areas. • Not properly verifying individuals by phone, in person, or in writing. • Not accounting for disclosures outside of treatment, payment or health care operations within the correct system, or manual process. 	<ul style="list-style-type: none"> • Re-training and re-evaluation. • Oral warning with documented discussion of policy, procedures, and requirements.
<ul style="list-style-type: none"> • Purposeful violation of privacy or an unacceptable number of previous violations. 	<ul style="list-style-type: none"> • Accessing or using PHI without having a legitimate need to do so. • Not forwarding appropriate information or requests to the privacy official for processing. 	<ul style="list-style-type: none"> • Re-training and re-evaluation. • Written warning with discussion of policy, procedures, and requirements.
<ul style="list-style-type: none"> • Purposeful violation of privacy policy with associated potential for patient harm. 	<ul style="list-style-type: none"> • Disclosure of PHI to unauthorized individual or company. • Sale of PHI to any source. • Any uses or disclosures that could invoke harm to a patient. 	<ul style="list-style-type: none"> • Termination.

Note: “PHI” is Protected Health Information as defined in policy number GC-009.