Privacy and Confidentiality

At MD Anderson, we are committed to safeguarding the privacy of our patients and workforce members, as well as safeguarding state resources. To such end, the protection of private and confidential information is an institutional priority.

Patient Information
Maintaining the confidentiality of protected health information (PHI) is driven by two of MD Anderson’s Core Values: Caring and Integrity. All uses and disclosures of PHI must be made with respect and sensitivity for our patients and the law. The most sensitive aspects of a patient’s life may be documented in the medical record, and understandably, this makes privacy and confidentiality a priority for our patients. Therefore, it is critical that all workforce members understand their role in maintaining the confidentiality of PHI and compliance with privacy laws.

Although the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the most recognizable privacy law, other federal and state laws play a significant role as well. In addition to violating MD Anderson policy, the inappropriate use or disclosure of PHI is a violation of federal and state law. Consequences for violations include jail time, monetary penalties, and disciplinary action, up to and including termination of employment.

PHI includes information related to:

- Diagnosis and treatment.
- Demographics, religious affiliation, and SSN.
- Family history, relationships, and genetics.
- Appointment schedule(s), birth date, admission date(s), and surgery date(s).
- Financial status, payment method(s), and insurance(s).
- Any other information attributed to an individual patient.

Uses and Disclosures of PHI

Privacy law requires that PHI only be used and/or disclosed for purposes of treatment, payment, or health care operations, unless a valid authorization is obtained from the patient, or as the law otherwise provides.

For example, accessing a friend’s PHI is not permitted unless you have a legitimate medical or business need, or a valid authorization from the patient. Uses and disclosures of PHI include: accessing PHI through any electronic systems; accessing PHI in paper format; printing, reading, or analyzing PHI; or discussing PHI with co-workers or anyone outside of MD Anderson.
Examples of impermissible uses and disclosures include, but are not limited to:

- Accessing a co-worker’s medical record to determine his diagnosis.
- Using the medical record, or any other information system to find a friend’s contact information (i.e., home address or telephone number).
- Disclosing PHI about a patient (celebrity or non-celebrity) to media outlets, or anyone else, without authorization from the patient.
- Using PHI in the medical record or any other MD Anderson database for research purposes without patient authorization and/or Institutional Review Board approval.

**E-mail**

Workforce members are discouraged from using e-mail to send PHI unless it is absolutely necessary for a medical or business purpose.

When using e-mail to send PHI, workforce members should review, understand, and follow MD Anderson’s Information Security Office Policy for the Use and Protection of Information Resources (Policy # ADM0335) and the Information Security Resources Security Operations Manual (see provisions regarding e-mail/data security).

Workforce members should remember:

- Internal e-mail communications containing PHI must be marked “Confidential.”
- External e-mail communications containing PHI should either be encrypted or be made through mymdanderson.org.

For more information related to e-mail or encryption, please contact the Information Security Office at 713-745-9000.

---

**Minimum Necessary Standard**

If PHI is used or disclosed for any purpose other than treatment, a minimum necessary determination must be made.

The Minimum Necessary Standard means determining what or who “needs to know.” In other words, for each use or disclosure made (with the exception of uses or disclosures made for treatment purposes), you must determine the smallest amount of PHI required to accomplish that purpose.

For example, if an employee needs assistance processing a patient’s financial forms, the employee may share the forms with a supervisor or co-worker. However, it would not be permissible to e-mail the forms to a large group with a general request for assistance. Disclosures of PHI must be limited to the minimum necessary to accomplish the purpose.
Patient Rights

Privacy law also establishes specific patient rights with regard to PHI, including the right to:

- Request a restriction on the use and disclosure of his or her PHI.
- Request an amendment to the designated record set.
- Request an alternative communication method.
- Inspect and copy the designated record set.
- Obtain an accounting of disclosures of PHI.
- Obtain either a paper or electronic copy of the Joint Notice of Privacy Practices.

HITECH Notification Requirements: Discovery of a Breach of PHI

Pursuant to federal law, MD Anderson is required to notify any individual whose PHI may have been breached. Generally any unauthorized access, use, or disclosure, which compromises the security or privacy of the PHI, would constitute a breach. Notice to the individual must be given without unreasonable delay, and in any case no later than 60 days from the date any MD Anderson workforce member discovered the breach.

Therefore, it is critical that any known or suspected breach be reported to the Institutional Compliance Office immediately.

Privacy Related Policies, Procedures, and Guidance

To assist with understanding and complying with privacy laws, MD Anderson has developed and implemented specific policies, procedures, and forms related to privacy. These documents are available through the Institutional Policies and Procedures Database. For more information regarding specific policies, procedures, and forms related to privacy, as well as additional guidance, frequently asked questions and other resource guides regarding the use and/or disclosure of patient information, see the Institutional Compliance Office intranet page at: http://inside.mdanderson.org/departments/privacy-compliance/.

If you have a privacy-related concern or question, contact the Institutional Compliance Office at 713-745-6636 or the Privacy Hotline at 1-888-337-7497.

Social Security Numbers (SSNs)

Federal and state laws, as well as The University of Texas System Policies and Standards – UTS165: UT System Information Resources Use and Security Policy (UTS165) regulate acceptable uses and disclosures of SSNs. Protecting the confidentiality of SSNs is critical to prevent identity theft and fraud.

To that end, MD Anderson workforce members are required to:

- Reduce the use and collection of SSNs.
- Inform individuals when SSNs are collected.
- Reduce the public display of SSNs.
- Control access to SSNs.
- Protect SSNs with security safeguards.
- Establish accountability for protecting the confidentiality of SSNs.

For more information regarding the use and/or disclosure of SSNs, see the Institutional Compliance Office intranet page at: http://inside.mdanderson.org/departments/privacy-compliance/.

MD Anderson’s Information

Much of the information obtained, developed, or produced by MD Anderson’s workforce members, as well as information supplied by outside entities for the benefit of MD Anderson, is considered confidential and/or proprietary. This information should not be disclosed to anyone outside MD Anderson, or used for personal benefit or gain, unless you have specific authorization to do so.
It is a violation of MD Anderson policy to:

- Share your user ID (login) and password for any MD Anderson system.
- Make any unauthorized inquiry, transmission, printing, or release.
- Breach the confidentiality of any data contained on any MD Anderson system.

Always take reasonable steps to prevent unauthorized use or disclosure of copyrighted, trademarked, or licensed materials and to safeguard MD Anderson information.

**Facility Information**

Information related to MD Anderson’s facilities, including files or documents that describe or identify the building or room name, location, type, purpose, or any negotiated contract pricing in any format are considered confidential. Such facility information must be protected from unauthorized access, use, disclosure, and/or dissemination. Specific facility information may relate to:

- floor plans;
- design plans;
- schematic plans;
- site plans;
- building and/or room specifications; or
- any such image.

For more information regarding protecting MD Anderson’s information, see MD Anderson’s Intellectual Property Policy (Policy # ADM0345), the Texas Public Information Act located in Chapter 552 of the Texas Government Code, and/or the Office of Technology Discovery intranet page at: http://inside.mdanderson.org/departments/technology-discovery/.

**Information Collected from the Public**

In accordance with state law, MD Anderson workforce members must include the following notice when collecting information from the public by means of a form (either electronic or paper):

- With few exceptions, the individual is entitled on request to be informed about the information MD Anderson collects about the individual.
- Under Sections 552.021 and 552.023 of the Texas Government Code, the individual is entitled to receive and review the information.
- Under Section 559.004 of the Texas Government Code, the individual is entitled to have MD Anderson correct information about the individual that is incorrect.

**Document Retention**

All information obtained, developed, or produced by MD Anderson's workforce members should be maintained in compliance with MD Anderson’s document retention schedule.

For more information regarding document retention, see MD Anderson’s Records Management Policy (Policy # ADM0107) or the Records Management Department intranet page at: http://inside.mdanderson.org/departments/records-management/.
**Questions and Answers**

**Question:** I carry an MD Anderson laptop between my office and my home, and I also take it with me on business trips. I use the laptop to store PHI related to my work, so I try and keep an eye on it at all times. Is there anything more I need to do to safeguard the information contained on/in the laptop?

**Answer:** Yes. MD Anderson’s Information Security Office Policy for the Use and Protection of Information Resources (Policy # ADM0335) requires that any mobile media device used to store PHI must be encrypted. This includes laptops, flash drives, PDAs, etc. For more information about safeguarding mobile media, please contact the Information Security Office at 713-745-9000. Additionally, if you ever lose a mobile media device that contains PHI or suspect that any information has been breached, please contact the Institutional Compliance Office immediately at 713-745-6636.

**Question:** I am a nurse and I noticed that a neighbor is scheduled to have a medical procedure. May I tell her other friends so that we can all support her in her time of need?

**Answer:** No. Although this seems like a supportive gesture, it is important to respect your neighbor’s privacy. You should not mention to your neighbor or other friends that you are aware of her condition. In addition, if you are not directly involved in the patient’s care, you should not access the patient’s medical record at all. It is a violation of MD Anderson policy and federal law to access a patient’s information without a legitimate medical or business need.

**Question:** Two employees are talking in the elevator. They start talking about a patient and seem to be talking about confidential information. What should you do?

**Answer:** Politely tell them that you are uncomfortable with their conversation because patient information is confidential. You can help protect patient privacy and confidentiality by following MD Anderson’s Confidentiality Policy (Policy # ADM0264). Our core values of caring and integrity depend upon every employee doing his/her part to protect patient privacy.
Patient Privacy: Right to Receive Accounting of Disclosures Policy (Policy # ADM0392)

Advertising Placement Policy (Policy # ADM0351)

Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (Policy # ADM0396)

Business Associate Agreement Policy (Policy # ADM0342)

Confidentiality Policy (Policy # ADM0264)

Disciplinary Action Policy (Policy # ADM0256)

Disposal of Patient Information Policy (Policy # ADM0389)

Family and Friends Blood Program Policy (Policy # CLN0535)

Patient Privacy: Fundraising Policy (Policy # ADM0162)

Patient Privacy: Notice of Privacy Practices Policy (Policy # ADM0396)

Marketing Mailing List Policy (Policy # ADM0352)

Patient Privacy: Uses and Disclosures of Protected Health Information Policy (Policy # ADM0401)

News Media Assistance Policy (Policy # ADM0414)

Non-Retaliation Policy (Policy # ADM0254)

Patient Privacy: Marketing and Advertising Policy (Policy # ADM0353)

Patient Privacy: Right to Request Amendment of Medical and Billing Records Policy (Policy # ADM0390)

Patient Privacy: Right to Inspect and Copy Medical and Billing Records Policy (Policy # ADM0391)

Patient Privacy: Right to Request Restrictions Policy (Policy # ADM0393)

Retention of Medical Records Policy (Policy # ADM0386)

Patient Privacy: Disclosures of a Patient’s Protected Health Information to Individuals Involved in the Patient’s Care Policy (Policy # ADM1032)

Patient Privacy: Breach Notification Policy (Policy # ADM1033)

Use of Alias and Confidentiality Flag Policy (Policy # ADM0978)