

Medical Student Registration Packet

Clinical rotations are geared for junior and senior level students only

Welcome to MD Anderson Cancer Center. We look forward to having you join our team for a truly unique and meaningful rotation experience.

As part of our vetting process, the Department of Trainee & Alumni Affairs (TAA) will require the following institutional forms at least 3 weeks before your rotation start date. Forms may be emailed or faxed to 713-792-7895.

- Medical Student Biographical Data Form
- Confidentiality Agreement Form
- IT User Acknowledgement Agreement Form
- HIPAA Exam and Acknowledgment Page
- *MD Anderson Standards of Conduct: Do the Right Thing* Acknowledgement Card
- **Medical Student Research Acknowledgment (only required for research rotations)**

Upon your arrival, please provide a form of photo identification (your current program ID or driver's license will suffice). You will receive a set of instructions for obtaining an MD Anderson badge.

Our office is located at:

1400 Pressler (@ Braeswood)
T. Boone Pickens Academic Tower - Suite 7.5000
Houston, TX 77030

Should you require additional information or have any questions, please feel free to contact us.

Sincerely,

Jana Mills
Program Manager
713-563-4321
jmills@mdanderson.org

Alma Hernandez
Sr. Academic Coordinator
713-563-8859
achernan@mdanderson.org

Sarah Broussard
Administrative Assistant
713-794-5814
sgbrouss@mdanderson.org



**Medical Student
Biographical Data Form**

MDA Department _____ Start Date _____ End Date _____

Full Name: _____
Last or Family First Middle Maiden

Current Address: _____

City State Zip Country

Preferred Email address: _____ Daytime Phone: _____

Social Security Number: _____ Date of Birth (mo/day/year): _____

Sex: M F

US Citizen Non-US Citizen

Naturalized Country of Birth _____ Visa Type _____

Voluntary (Ethnic Origin):

American Indian/Native American Black, Non-Hispanic White Asian
 Native Hawaiian or other Pacific Islander Hispanic of any race Two or more races

List medical school of current enrollment

Name of Institution City/State	Start Date (mo/day/yr)	Expected Graduation (mo/day/yr)

Acknowledgement Social Security Disclosure Notice

Disclosure of your social security number ("SSN") is requested as part of the process for educational appointment with The University of Texas MD Anderson Cancer Center ("MD Anderson"). During the educational appointment process, your SSN will be used as a unique number to identify you within MD Anderson's current tracking system. Federal law requires MD Anderson to report income and SSNs for all trainees to whom compensation is paid and/or for whom background and sanction checks are performed. The SSN is also used for purposes of payroll, benefits, internal verification, administrative purposes, and to verify appointment. MD Anderson reports SSNs to Federal and State agencies or their contractors as authorized or required by law and for benefits purposes. Further disclosure of your SSN is governed by the Public Information Act (Chapter 552 of the Texas Government Code) and other applicable law.

Acknowledgement Statement

I acknowledge the above statements and all other information otherwise given by me as true, complete and not misleading in any way. I understand that any incorrect, incomplete, misleading, or false statements furnished by me will result in discharge. As part of my rotating appointment, I agree to comply with all rules, regulations, and policies of The University of Texas MD Anderson Cancer Center.

Signature: _____

Date: _____



Confidentiality Agreement Trainee and Alumni Affairs

I _____
(Trainee Name)

a trainee of _____
(Name of University, School or Institution)

am assigned to utilize the facilities of The University of Texas M. D. Anderson Cancer Center in order to gain educational experiences. In consideration of this educational opportunity, I agree and promise I will:

1. maintain and preserve the confidences of patients and information in records;
2. **NOT** disclose or divulge confidential material or information of any kind;
3. **NOT** publish any writing relating to my experience as an extern at The University of Texas M. D. Anderson Cancer Center, without the prior written approval of my supervisor at the Cancer Center; and
4. adhere to The University of Texas System Rules & Regulations, including the institutional intellectual property policies.

Signature of Trainee Date

1515 HOLCOMBE BOULEVARD • HOUSTON, TEXAS 77030-4095 • 713-792-2121 • www.mdanderson.org

A Comprehensive Cancer Center designated by the National Cancer Institute
located in the Texas Medical Center

The University Of Texas M. D. Anderson Cancer Center
INFORMATION RESOURCES ACCEPTABLE USE AGREEMENT AND USER ACKNOWLEDGEMENT
OFFICE OF TRAINEE & ALUMNI AFFAIRS

The University of Texas M. D. Anderson Cancer Center (“M. D. Anderson”) relies on information resources and the data contained within those systems to achieve its mission. This Acceptable Use Agreement protects these resources in accordance with regulatory requirements and M. D. Anderson policies and practices. All individuals granted access to Information Resources must follow the acceptable use rules below:

A. General	<ul style="list-style-type: none"> • M. D. Anderson information resources are provided for the express purpose of conducting the business and mission of M. D. Anderson. • Information stored on M. D. Anderson information resources may only be shared with others who have a business need to know such information, and such information may only be shared in compliance with applicable laws, regulations, and policies. • M. D. Anderson information resources must not be used to: engage in acts against the mission and purposes of the Institution, intimidate or harass, degrade performance, deprive access to an institution resource, obtain extra resources beyond those allocated, or to circumvent security measures. • Information resources must not be used to conduct a personal business or used for the exclusive benefit of individuals or organizations that are not part of The University of Texas System. Any exceptions must be in support of M. D. Anderson missions and require the prior written approval of an Executive Officer of M. D. Anderson. Incidental personal use of certain systems is permitted (refer to Section F below). • Obscene materials must not be intentionally accessed, created, stored or transmitted. • Users must not copy or reproduce any licensed software except as expressly permitted by the software license, use unauthorized copies on M. D. Anderson-owned computers or use software known to cause problems on M. D. Anderson-owned computers. • Any exception to the acceptable use of information resources must be approved by the Information Security Department.
B. Data Protection	<ul style="list-style-type: none"> • Any information concerning any person, system, or asset of M. D. Anderson that is obtained in the performance of one’s duties is of value to M. D. Anderson and may be confidential or restricted confidential and shall not be disclosed to any individual, unless such release of information is directly related to the performance of one’s responsibilities. • Data will be accessed on a need-to-know basis. Users of M. D. Anderson information resources must not attempt to access data or programs contained on resources for which they do not have authorization or consent. • All critical data (electronic files) will be saved on network servers to ensure backup of the data. All data, including research data, shall be backed up for disaster recovery purposes. • All records (electronic or paper) will be maintained in accordance with the M. D. Anderson Records Retention Policy.
C. Virus Protection	<ul style="list-style-type: none"> • All computers connecting to the M. D. Anderson network must run current and authorized virus prevention software. Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other special circumstance. Computers found to be infected with a virus or other malicious code may be disconnected from the M. D. Anderson network until deemed safe by the Information Security Department.
D. Electronic Mail	<ul style="list-style-type: none"> • The following electronic mail (email) activities are prohibited: <ul style="list-style-type: none"> - Using email for purposes of political lobbying or campaigning except as permitted by the Regents' Rules and Regulations. - Posing as anyone other than oneself when sending email. - Reading another user's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services. - Use of email software that poses a significant security risk to other users on the M. D. Anderson network. - Sending or forwarding “chain” letters. - Sending unsolicited messages to large groups except as required to conduct M. D. Anderson business. - Sending excessively large messages or attachments unless in performance of official M. D. Anderson business. - Knowingly sending or forwarding email that is likely to contain computer viruses.
E. Confidential or Restricted Confidential Information	<ul style="list-style-type: none"> • All Confidential and Restricted Confidential information (e.g. Protected Health Information, Sensitive Research Data, student Data, Social Security Numbers) transmitted through open networks (e.g., the Internet and wireless) must be encrypted in accordance with M. D. Anderson Encryption Guidelines. This information must not be sent or forwarded to non-M. D. Anderson email accounts, unless encrypted. Refer to Information Security web-site for Data Classification Guidelines & Ratings.
F. Incidental Personal Use of Information Resources	<ul style="list-style-type: none"> • Incidental personal use of electronic mail and internet access is permitted by M. D. Anderson policy but is restricted solely to authorized users (authorization does not extend to family members or other acquaintances). Incidental personal use must not interfere with normal performance of an employee’s duties, must not result in direct costs to M. D. Anderson, and must not expose M. D. Anderson to unnecessary risks. • Storage of any non-work related email messages, files and documents within the M. D. Anderson email system

	<ul style="list-style-type: none"> must be nominal (less than 5% of a user's allocated mailbox space). Non-work related information may not be stored on network file servers. All messages, files and documents stored on M. D. Anderson computing resources—including personal messages, files and documents) are owned by the institution in accordance with the Regents' Rules and Regulations and are subject to M. D. Anderson review. Any files, messages or documents residing on M. D. Anderson computers may be subject to public information requests and may be accessed in accordance with M. D. Anderson policy.
G. Internet Use	<ul style="list-style-type: none"> Software for browsing the Internet is provided to authorized users for business, education, research, and patient care purposes. Due to network maintenance and performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review. Email or postings by users of M. D. Anderson network resources to news groups, "chat rooms" or "listservs" must not give the impression that they are representing, giving opinions, or making statements on behalf of M. D. Anderson, unless authorized. Faculty and staff members shall use a disclaimer stating that the opinions expressed are their own and not necessarily those of M. D. Anderson. Personal commercial advertising must not be posted on M. D. Anderson web sites.
H. Portable and Remote Computing	<ul style="list-style-type: none"> All computers and portable-computing devices accessing M. D. Anderson information resources must be password protected in accordance with M. D. Anderson policy. At a minimum, such passwords are to be changed at least every 90 days, or immediately if there is suspicion that the password has been compromised. Users accessing the M. D. Anderson network from a remote computer must adhere to all policies that apply to access from within the local campus network. Remote computers are subject to the same rules and security related requirements that apply to M. D. Anderson-owned computers. Unattended portable computing devices must be physically secured. If it is determined that required security related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber attack or in some way endangers the security of M. D. Anderson, the account and/or network connection will be disabled. Access will be re-established once the computer or device is determined to be safe by M. D. Anderson. Users must not divulge M. D. Anderson dialup or modem phone numbers to anyone. If confidential or protected M. D. Anderson data is stored on portable computing devices, it must be encrypted and backed up to a network server for recovery in the event of a disaster or loss of information. Special care shall be taken to protect information stored on laptops and personal digital appliance (PDA) devices, and in protecting such devices from theft.
I. Passwords	<ul style="list-style-type: none"> Every M. D. Anderson computer/network account, password, any personal identification number (PIN), digital certificate, security token (<i>i.e.</i>, Smartcard), or any other similar information or device used for identification and authorization purposes, must not be shared. Each user of M. D. Anderson resources is responsible for all activities conducted using his or her account(s). Users must not circumvent password entry through use of auto logon, application "remember password" features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (such as automated backup and single sign-on solutions) with the approval of the Information Security Department. Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction. (For more information, see the Password Guidelines.)
J. Security	<ul style="list-style-type: none"> Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems shall not be downloaded and/or used, except as authorized by the Information Security Department. For example, password cracking programs, packet sniffers, or port scanners on M. D. Anderson information resources shall not be used. Users must report any identified weaknesses in M. D. Anderson computer security and any incidents of possible misuse or violation of this agreement to an immediate supervisor, department head, or the Information Security Department. Where technically feasible, all PC's, laptops, PDA devices and workstations shall be secured with a password-protected automatic logoff feature set at 15 minutes or less to prevent unauthorized access to the device. Media containing confidential or restricted confidential information must be used, reallocated and disposed of in such a manner as to prevent unauthorized access to the data.

User Acknowledgement – Trainee

I acknowledge that I have received and read the M. D. Anderson Information Resources Acceptable Use Agreement stated above. I understand that this document will be maintained as a permanent record in my trainee file, that I must comply with this agreement and other M. D. Anderson policies related to the use of any data or information and all information systems, and that my failure to do so may result in appropriate disciplinary action up to and including termination and/or action by law enforcement authorities.

Signature: _____ Date: _____

Print Name: _____ Trainee ID # _____

stitutional COMPLIANCE



professional organizations and all hearings, including financial and accounting matters, in accordance with high standards of business and ethical conduct.

Principle Three:

Maintain M. D. Anderson's confidential, business, proprietary, and protected information in a manner that meets all applicable laws, rules, guidelines, and document retention schedules.

Principle Four:

Refrain from: (a) soliciting or accepting gifts, favors, benefits, services, or items of value in return for preferential treatment or patient referrals; or (b) offering or paying to anyone gifts, favors, benefits, services, or items of value in return for patient referrals.

Principle Five:

Provide, document, and bill for services in a manner that reflects the utmost ethical and legal conduct.

Principle Six:

Refrain from using M. D. Anderson resources, including time, funds, equipment, or other resources in a wasteful manner; for personal benefit or gain; to harm another person; for political activity; or for illegal activity.

Principle Seven:

Act with honesty and good faith in all matters, and refrain from engaging in discriminatory, harassing, retaliatory, or inappropriate behavior.

Principle Eight:

Refrain from soliciting or accepting anything that might influence, is being offered with the intent to influence, or might reasonably appear to influence your official duties. Refrain from engaging in activities or entering into contracts that could or could reasonably appear to: (a) interfere with your responsibilities to M. D. Anderson; (b) require or induce you to disclose confidential information obtained from or through M. D. Anderson; or (c) impair your independent judgement.

Principle Nine:

Conduct all research in a manner consistent with applicable legal, ethical, and professional requirements, as well as M. D. Anderson policies and procedures.

Principle Ten:

Notify the Chief Compliance Officer promptly of any suspected or discovered breach of this Institutional Code of Conduct and cooperate fully with all inquiries and investigations related to a breach.

Please contact the Institutional Compliance Office for any questions related to the disclosure of protected health information.

Privacy Hotline 1-888-337-7497

Institutional Compliance Office 713-745-6636

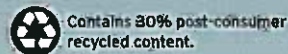
Fraud & Abuse Hotline 1-800-789-4448

Chief Compliance Officer via the page operator 713-792-7090

Institutional Compliance Office • Unit 640

The University of Texas M. D. Anderson Cancer Center

P.O. Box 301402 • Houston, TX 77230-1402



stitutional COMPLIANCE



THE UNIVERSITY OF TEXAS
MD ANDERSON
CANCER CENTER
Making Cancer History®

At M. D. Anderson, protecting our patients' privacy is a high priority. Everyone who enters this campus must do his/her part to respect our patients and their information by being aware of the sensitive nature of this environment. M. D. Anderson has developed a comprehensive Privacy Compliance Program within the Institutional Compliance Office to ensure that Protected Health Information ("PHI") is managed with the highest levels of respect and confidentiality. Part of that effort involves education on state and federal privacy laws (e.g., the Health Insurance Portability and Accountability Act and M. D. Anderson's privacy policies and procedures).

This training is an institutional requirement for your interactions with the institution and/or your short-term program. Please

What is Protected Health Information ("PHI")?

PHI is any individually identifiable health information that is directly related to a person's past, present, or future health care. For example, PHI includes: name, address, Social Security number, photos, dates of service, date of birth, contact information, medical record numbers, diagnosis, financial/payment information, and provider information. PHI includes individually identifiable health information whether it is electronic, on paper, or spoken word. See "Confidentiality Policy" (Policy # ADM0264).

What is the General Rule of Privacy?

In general, PHI may be used or disclosed for purposes of treatment, payment, or health care operations ("TPO") without authorization. For example, with no specific authorization providers are permitted to consult with one another about a patient, or a hospital can exchange information with the patient's insurance company.

For uses or disclosures other than TPO, a specific patient authorization is required. The authorization must contain specific elements and be obtained in compliance with M. D. Anderson's policy. See "Authorization for the Use and Disclosure of Protected Health Information (PHI) Policy" (Policy # ADM0396).

Minimum Necessary Standard.

The minimum necessary standard means determining what should be used or disclosed or who "needs to know." In other words, for each use or disclosure made, you must determine the smallest amount of PHI necessary to accomplish that purpose. This standard requires you to limit both the amount of PHI and the number of persons involved in its use or disclosure. (EXCEPTION: The minimum necessary standard does not apply to treatment-related uses or disclosures). See "Confidentiality Policy" (Policy # ADM0264).

Other Privacy Issues.

Other privacy issues that you should be aware of include (but are not limited to) the following:

Security of Electronic Information:

Although privacy protection applies to both electronic and paper-based PHI, there are some specific rules that apply to electronic information at M. D. Anderson. These include access rights, encryption standards, and internet content monitoring. There are also specific procedures related to accessing, e-mailing, or faxing PHI. See "Information Security Office Policy for the Use and Protection of Information Resources" (Policy # ADM0335).

Patient Rights:

The Privacy Rule created many new rights for patients including rights: to access and copy the medical record, request amendments to the medical record, and to obtain an accounting of disclosures of PHI. These are explained to patients during the registration process through document titled "M. D. Anderson's Joint Notice of Privacy Practices." See "Notice of Privacy Practices (NPP): Distribution and Acknowledgement Policy" (Policy # ADM0395).

Disposal of PHI:

Proper disposal of PHI is critical to maintaining patient confidentiality. When disposing of PHI in paper format, be sure to place it in the designated bins. Do not leave paper PHI out in public view or in unlocked drawers. Do not dispose of paper PHI in regular trash cans or recycling bins. Always remove PHI from any conference, meeting, or education event before leaving the room. See "Disposal of Confidential and/or Sensitive Information Policy" (Policy # ADM0389), and "Information Security Office Policy for the Use and Protection of Information Resources" (Policy # ADM0335).

What Privacy Rules Apply?

The Health Insurance Portability and Accountability Act (HIPAA) is the primary federal law regulating PHI, however many other federal and state laws also apply. Noncompliance with any of these laws can result in both civil and criminal penalties. Under HIPAA, civil penalties can be as high as \$25,000 per identical violation, and criminal penalties can be as high as \$250,000 and/or a 10-year prison sentence.

M. D. Anderson requires compliance with all Institution policies and procedures, including those that define the way PHI may be used and disclosed at M. D. Anderson. Noncompliance with M. D. Anderson's Institutional policies and procedures may result in penalties and disciplinary action, up to and including termination or expulsion.

Ways You Can Protect Patient Privacy.

Be aware that in your program you may have access to PHI. Your access might be direct (e.g., review of patient cases, being present during an exam), or it might be indirect (e.g., seeing patients in the clinical setting, or listening to medical staff as they perform their jobs). In either case, it is your responsibility to keep the PHI confidential. Never repeat PHI that you hear or see while at M. D. Anderson. Do not discuss PHI with co-workers, friends, neighbors, or your family unless they are directly involved in the care of that patient. I

Acknowledgement Card

I attest that I have read the HIPAA Privacy Education brochure and completed the exam. I understand that the brochure highlights laws, policies, rules, and regulations applicable to The University of Texas M. D. Anderson Cancer Center. I further understand that compliance with these laws, policies, rules, and regulations is mandatory, and I agree to adhere to M. D. Anderson's policies and procedures with respect to any PHI that I come into contact with while at M. D. Anderson.

Signature

Printed Name

Date

Exam

Please complete the following exam, and then sign and date the acknowledgement card on the reverse side of the exam. You will need to return the exam and acknowledgement card to your program director/coordinator before you participate in the program. Please retain the rest of the brochure to use as a reference during your time at M. D. Anderson.

While at M. D. Anderson you notice that your friend is a patient. The friend has not told anyone she is being treated for cancer and does not know that you have seen her here. What should you do?

- Call her as soon as you get home, and ask if she needs any help.
- Try and find out more about her diagnosis by following her to her clinic, or accessing her medical record.
- Respect her privacy by not telling anyone else, and by not talking to her about it unless she volunteers the information first.
- All of the above.

PHI includes information related to diagnosis and treatment, financial status, and height and weight measurements.

- True.
- False.

When disclosing patient information to another provider for the purpose of treatment, you must limit the PHI disclosed to the minimum necessary to achieve the purpose.

- True.
- False.

If you are given paper (e.g., presentations, handouts, summaries, case histories, etc.) that contains PHI, what is the best way to dispose of the paper when you have finished with it?

- Leave the paper on the table because the staff will come by and properly dispose of it after you have left.
- Place it in a recycle bin.
- Place it in a bin designated for the disposal of PHI.
- Shred the paper at home.

If you are unsure whether you are using or disclosing PHI in an appropriate manner, whom should you contact?

- The patient whose PHI is being used or disclosed.
- The Institutional Compliance Office at (713) 745-6636.
- Patient Advocacy at (713) 792-7776.
- The business center in your clinic.

Acknowledgement Card

I certify that I have received, read, and agree to abide by the *MD Anderson's Standards of Conduct: Do the Right Thing* booklet. I understand that the booklet represents laws, policies, rules, and regulations applicable to The University of Texas MD Anderson Cancer Center. I understand that compliance with these laws, policies, rules and regulations is mandatory.

Signature

Printed Name

Employee ID Number

Date

[MD Anderson's Standards of Conduct: Do the Right Thing Booklet](#)



Medical Student Research Acknowledgement

Rotating Research Medical Students have the following privileges and restrictions:

Rotating Research Medical Students may:

- participate in a supervised research project/paper;
- be a single author or first author on a manuscript with the approval of the mentor;
- attend conferences and lectures;
- have 'view-only' access to MD Anderson clinical systems (i.e. ClinicStation)

Rotating Research Medical Students may not:

- Have any patient contact while in a research role;
- Write in the medical chart;
- Order tests or services;
- Participate in decisions concerning management of a patient;
- Render treatment or other patient services;
- Perform a primary medical evaluation or a history and physical;
- Obtain informed consent for participants/patients related to any procedure or protocol;

Your appointment is contingent upon your consistent demonstration of satisfactory performance and behavior as defined by the mentor/program/department to which you are assigned.

Your activities at this institution are governed by The UT System Rules and Regulations, including the institutional Intellectual Property Policy (Policy ADM0345). You will be expected to maintain the confidentiality of University proprietary information, and to obtain approval from your chair/mentor/program director prior to disclosing or publishing any results of your activities at MD Anderson. Please refer to the Scientific Publications Policy for standards on publishing papers and/or manuscripts. (Policy ACA0018).

MD Anderson is committed to conducting research that is unbiased and in compliance with federal and state laws, rules, and guidelines, as well as institutional policies regarding conflict of interest. To facilitate the research compliance review process, there is an electronic application through which faculty, trainees, supervisors, and institutional decision makers electronically submit disclosures of potential conflicts of interest and a series of compliance checks relevant to the type of disclosure relative to the Conflict of Interest Policy (Policy ACA0001). You will receive an MD Anderson Outlook account upon starting your research rotation to fulfill this requirement.

I have read and understand the above guidelines and restrictions of the Rotating Research Medical Student appointment:

Printed Name:

Signature

Date