Methodist Healthcare System
Graduate Medical Education
Rotator On-boarding Checklist

❗ New Innovations(NI) assigned items:

New Rotators

MHS GME Policy Review – (Please check “reviewed” box for all policies provided; all sponsoring institutions)

Rotating Resident Checklist:

☐ Emergency Contact Form
☐ Security Access Form (Highlighted fields only)
☐ Confidentiality & Security Agreement
☐ Rotating Resident Acknowledgement
☐ Electronic Signature Agreement

☐ Letter of good standing from current program (obtain from program coordinator)
☐ Curriculum Vitae (CV)
☐ Immunization Records (must be official; print screens, word or excel documents are not accepted)
☐ Proof of Negative Tb Test within last 12 months(*annual) or Chest X-Ray (official results report; valid 5yrs)
☐ Proof of current season Flu vaccine (*annual)
☐ National Provider Identifier (NPI) (print screen from NPI registry website)
☐ Copy of TX Medical License or PIT – Physician in Training Permit
☐ Copy of Malpractice Certificate – Military N/A (obtain from program coordinator)
☐ Copy of ECFMG Certificate (if applicable; IMG only)
☐ Copy of ACLS/ATLS/BLS/PALS Life Support Card (*valid, front, back with signature)
☐ Copy of Board Certification (if applicable)
☐ Copy of Photo ID (*valid; must be State or Federal issued)

*valid/annual–may be requested annually or upon renewal

❗ Please note; all items above will be completed electronically, via MHShealth New Innovations(NI) Notification with instructions, site link and log on credentials will be sent to each new rotator
New Innovations(NI) assigned items:

Returning Rotators

MHS Returning Acknowledgement *(MHS GME Policy Review)*

Returning Resident Checklist:

☐ Letter of good standing from current program *(obtain from program coordinator)*
☐ Copy of Malpractice Certificate – Military N/A-*annual* *(obtain from program coordinator)*
☐ Curriculum Vitae (CV)
☐ Immunization Records *(must be official; print screens, word or excel documents are not accepted)*

☐ Proof of Negative Tb Test within last 12 months-*annual* or Chest X-Ray *(official results report; valid 5yrs)*
☐ Proof of current season Flu vaccine *(annual)*
☐ Copy of ACLS/ATLS/BLS/PALS Life Support Card *(valid, front, back with signature)*
☐ Copy of Photo ID *(valid; must be State or Federal issued)*

*valid/annual–may be requested annually or upon renewal

Please note; all items above will be completed electronically, via MHShealth New Innovations(NI)
Notification with instructions, site link and log on credentials will be sent as necessary for returning rotators
Methodist Healthcare Graduate Medical Center
Emergency Contact Information

**Personal Information**
Name (Last, First): ________________________________
Address: ________________________________
Phone/Cell Number: ________________________________
Pager Number: ________________________________
Personal email address: ________________________________
Status (faculty/staff/student/resident/fellow): ________________________________
Specialty: ________________________________
Supervising Faculty: ________________________________

**Emergency Contact**
Name of Emergency contact (Last, First): ________________________________
Telephone Number of Emergency contact: ________________________________
Cell phone you will use if you evacuate: ________________________________
**Methodist Healthcare System**

**REMOTE ACCESS REQUEST FORM**

Questions? Call 210-575-0090
Please fax completed form to 210-510-6018

---

**Your Information (Please Print - * Required Fields - necessary for account creation and verification):**

<table>
<thead>
<tr>
<th>First Name: *</th>
<th>Middle Initial *</th>
<th>Last Name: *</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practice Address: *</th>
<th>City, State, Zip: *</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSN *</th>
<th>Date Of Birth: *</th>
<th>3-4 User ID [if known]:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone: *</th>
<th>Ext:</th>
<th>Fax:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practice Name:</th>
<th>Specialty:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Are you a physician?**

- [ ] Yes

**If yes, degree? (MD, DO, etc.)**

**Are you credentialed with Methodist Healthcare System?**

- [ ] Yes

**To which applications would you like access**

- Meditech
- Radiology PACS

**Please list all physicians, groups, or insurance (if applicable) to which you will require access:**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**User Signature: _______________________________ **

<table>
<thead>
<tr>
<th>Date: __________________________</th>
</tr>
</thead>
</table>

I understand that the password assigned to me for accessing the above designated application(s) is to be held in STRICT CONFIDENCE, cannot be shared with other users, and is only to be used in the manner designated in the appropriate procedures. I also understand that willful discharge of mine or any other user’s password, misuse of my password, or use of another’s password can be grounds for revocation of access.
Provider Confidentiality and Security Agreement

Note: this form to be used for non-employed physicians, providers and their non-HCA-employed staff.

I understand that the HCA affiliated facility or business entity (the “Company”) at which I have privileges or for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients’ health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, “Confidential Information”).

In the course of my affiliation or employment with the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company’s Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company provided systems.

General Rules

1. I will act in accordance with the Company’s Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company’s policies.
4. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
5. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
6. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility’s medical staff, I may no longer use the facility’s equipment to access the Internet.

Protecting Confidential Information

7. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
8. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
9. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
10. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
11. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
12. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

13. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services at this facility, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
14. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient’s record or Company information, I am
affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

15. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.

16. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

17. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (e.g., PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.

Doing My Part – Personal Security

18. I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.

19. I will ensure that members of my office staff use a unique identifier to access Confidential Information.

20. I will:
   a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
   b. Use only approved licensed software.
   c. Use a device with virus protection software.

21. I will never:
   a. Disclose passwords, PINs, or access codes.
   b. Use tools or techniques to break/exploit security measures.
   c. Connect unauthorized systems or devices to the Company network.

22. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and positioning screens away from public view.

23. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
   a. my password has been seen, disclosed, or otherwise compromised
   b. media with Confidential Information stored on it has been lost or stolen;
   c. I suspect a virus infection on any system;
   d. I am aware of any activity that violates this agreement, privacy and security policies; or
   e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

24. I agree to notify my Physician Support Coordinator within 24 hours, or the next business day, when members of my office staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.

25. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.

26. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.

27. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

<table>
<thead>
<tr>
<th>Provider Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Printed Name</td>
<td></td>
</tr>
</tbody>
</table>
Rotating Resident Acknowledgement

- You are required to wear your white lab coat at all times while on the premises of Methodist Healthcare System Hospitals as well as your Program assigned badge.
- Identification badges are to be worn on the upper portion of the chest on the outer garment (except in areas where a sterile environment is required).
- Residents are required to identify themselves as such with each patient encounter as a resident and inform them that you are in training.
- E-mail is the official line of communication; residents will provide the GME office with a valid e-mail address and will check e-mail often.
- Residents will notify the GME office immediately if they test positive for TB during their rotation. Individuals who test positive for TB may not be present in any MHS facility and will not be permitted back until they submit documentation of a negative PPD test or chest x-ray.
- Residents will check in with the GME office by phone or in person on the first day of rotation for all non-consecutive rotations.
- Residents will park in areas designated by the GME Office, any parking violations are the Resident’s responsibility.
- Residents will not give their access cards to another individual to use; access cards are for individual use only and must be returned at the end of each training year.
- MHS is a total tobacco-free work environment beginning November 18, 2010.
- Residents will use electronic provider documentation (pDoc) in the Electronic Healthcare Record (EHR) for all patient documentation (except for some reports which can be dictated).
- Residents will submit all orders electronically using CPOE.
- Residents will limit the use of Telephone and Verbal Orders; residents should not admit patients using Telephone Orders.
- Residents will not use another physician’s computer login or dictation ID for any documenting purposes. You are required to complete computer training, orientation, and abide by the HIM rules for completion of medical records. **Failure to attend will result in a delay of rotation start.**
- Residents will complete all Medical Records within 5 business days after the end of rotation or their Program Director will receive a letter stating that the Resident did not adhere with Methodist Hospital standards while on rotation.
- Any manual signature by a resident at Methodist Health Systems will be in the following format:

  *Resident John Smith (Resident John Smith)/ Supervising Physician: John Physician, M.D.*
I have read and understand the contents of this acknowledgement and will act in accord with the items mentioned as a condition of my rotation with Methodist Healthcare System.

________________________
Resident Signature

________________________  __________________________
Resident Name (Printed)      Date
I, ________________________________ , wish to participate in the Electronic Signature Program to authenticate medical record reports and/or orders. The reports/orders will be electronically signed via the Hcare Horizon Patient Folder utilized at Methodist Healthcare.

The unique identifier (PIN) that has been assigned to me for purposes of electronic signature is official and confidential. I certify that I will not disclose the identifier assigned to me to any other person or permit another person to use it.

In the event I misuse the electronic signature, I understand that my use will be terminated and my PIN inactivated. Misuse as defined by CMS is “that the physician has allowed another person or persons to use his/her personally assigned identifier”

HCA security regulations state that a security violation exists when a user has allowed another person or persons to use his/her PIN. Security violations will be reported to the appropriate hospital committees and/or Administrative persons as addressed by facility security policies and procedures.

I agree to review each entry or document on-line prior to affixing my electronic signature. I understand that I am responsible for the content of all medical record entries that I authenticate electronically.

I agree to sign the Confidentially Agreement to use the Hcare Horizon Patient Folder

________________________________________
Resident Signature

________________________________________  __________________________
Resident Name (Printed)  Date