ROTATING & VISITING RESIDENT/STUDENT APPLICATION / REQUEST

Please complete ALL fields
MUST submit 30 business days prior to start date

Incomplete or unsigned agreements WILL NOT be accepted or processed and could result in delayed rotation start dates and access!

Effective September 1 2023, no other application/request forms for rotating residents/students will be accepted. *All applications must be filled in and no handwritten forms will be accepted.* In an effort to ensure the hospital is aware of Non-OUHSC residents rotating at OU Medicine, it will be the responsibility of the residency programs accepting the residents to notify the hospital by completing the information below and submitting it to Medical Staff Services. Please do not submit requests to any other department to request access or setup. Medical Staff Services will process this request and complete the processes for IT accesses and badges.

A complete application includes:

- All fields completed in this packet – pages 1 through 7.
- A copy of letter of good standing attesting applicant is currently enrolled in the program, is in good standing, has a recent background check, and has complied with all OUH vaccination requirements.
- A recent photo – program photo preferred (jpeg only)
- From Nov through May, must provide a copy of Flu documentation (vaccination or approved declination)
    - *If you have not received an Influenza Vaccination within the past year you must wear a mask in all patient care areas of the facilities during Flu Season (November 1 thru March 31)*
- If this is for a Med Student or Resident is doing research we must also have the Approved IRB (Internal Review Board) letter with the researcher's name listed also attached to the request.)
- Medical License (if applicable)
- DEA (if applicable)
- OUH Sponsor (Faculty, Bus Admin or Program Coord)– The OUH Sponsor MUST have an OUH ID. If the sponsor is not in the OUH system with an OUH ID, they must get an OUH ID BEFORE this form is submitted to Medical Staff Services. OUH Sponsor/Manager will need to open a request to get an OUH ID created prior to this form being submitted.

It will also be the responsibility of the Residency Programs and attending physicians accepting the residents to ensure before the rotation is complete that all medical records have been completed, otherwise it will be the responsibility of the attending physician to complete the medical record if the resident is no longer at OU Medicine.

Date

Taxonomy Code
If unknown, check https://npiregistry.cms.hhs.gov/search

Demographics

Last Name		First Name		Initials *If you only have 2 initials, use X as middle initial.*
DOB	SSN	Cell		
Home Address		City	State	Zip
Email	NPI		Medical Lic *If applicable*	DEA *If applicable*
Office Address *If applicable*		City	State	Zip
Office Email *If applicable*			Pager #	

Program Information

Name of Home School / Training Program			Dept where rotating
Name of Clinical Service			Location / Facility Where Rotating
OUH Sponsor First and Last Name *(MUST have OUH ID for sponsor to submit)*			Sponsor's OUH ID
Sponsor Phone		Sponsor Email	
Rotation Start Date	Rotation End Date		1. Previously rotated at OUH 2. Needs EPIC Access

Program Type (Job Role)

- ◯ MSIII
- ◯ Resident
- ◯ Fellow
- ◯ Psych Fellow
- ◯ Professional Enrichment Course (MSII)
- ◯ MSIV
- ◯ PA Student
- ◯ NP Student
- ◯ Pharm D Student
- ◯ Researcher (ONLY NON-EMPLOYED Student, Resident, Fellow, PA Student, NP Student researchers)

Return completed form to the Medical Staff Services Department Email credentialing@ouhealth.com

Student/Resident Access Request

Date	**Taxonomy Code** If unknown, check https://npiregistry.cms.hhs.gov/search

Demographics

Last Name	First Name		Initials *If you only have 2 initials, use X as middle initial.*
DOB	Cell		
Home Address	City	State	Zip
Email	NPI	Medical Lic *If applicable*	DEA *If applicable*
Office Address *If applicable*	City	State	Zip
Office Email *If applicable*		Pager #	

Program Information

Name of Training Program				Dept where rotating	
Name of Clinical Service *(i.e. OB/GYN)*				Location / Facility Where Rotating	
OUH Sponsor First and Last Name *(MUST have OUH ID for sponsor to submit)*				Sponsor's OUH ID	
Sponsor Phone		Sponsor Email			
Rotation Start Date	Rotation End Date			1. Previously rotated at OUH 2. Needs EPIC Access	

Program Type (Job Role)

- ◯ MSIII
- ◯ Resident
- ◯ Fellow
- ◯ Psych Fellow
- ◯ Professional Enrichment Course (MSII)
- ◯ MSIV
- ◯ PA Student
- ◯ NP Student
- ◯ Pharm D Student
- ◯ Researcher (ONLY NON-EMPLOYED Student, Resident, Fellow, PA Student, NP Student researchers)

- I have read the examples and understand Appropriate Access of patient information.
- I understand that if I or my family are patients, I should not access my own nor family records.
- I agree to look ONLY at patient information on a need-to-know basis to do my job.
- I will log off /exit all OU Health systems when I leave the terminal/computer.
- I understand it is against OU Health Policies and Procedures for software to be installed on a medical student's laptop or home computer.
- I understand that I should not use anyone else's OUH ID and password. I understand that Ishould not let anyone else use my OUH ID and password.

Requester Signature _____ Date _____

First Name

Last Name

OUH Service Desk
Phone: 405-764-8000
Internal Extension: 88000

Confidentiality and Security Agreement

I understand that OU Medicine, Inc. and its affiliated facilities and entities (collectively, "OUH" or the "Company") 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, credentialing, intellectual property, 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 in OUH's policy management system (https://hub.ouhealth.com/sites/home?cli=3748) (under the Policies and Procedures tab). 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 OUH medical staff, I may no longer use OUH'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 and Company record retention policy (provided upon request)
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 purging 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 OUH facilities, 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.*, OUH 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).
    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. Allow another individual to use my digital identity (e.g., OUH ID) to access, modify, or delete data and/or use a computer system.
    c. Use tools or techniques to break/exploit security measures.
    d. Connect unauthorized systems or devices to the Company network.
22. I will practice good workstation security measures such as locking up external media 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, Chief Information Security Officer, Chief Technology Officer, or OUH service 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 the OUH IT Department 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.

Requester Signature _____ Date _____

First Name

Last Name

APPROPRIATE ACCESS
Systems User's Guide

CONFIDENTIALITY...

OUR POLICY: We have an ethical obligation to protect the confidentiality of our patients and theirmedical information. OUH systems should be used appropriately; that is, to access information only as necessary to do your job. Please review the following examples:

APPROPRIATE ACCESS:

- **Review the Electronic Signature Policy.**
- **Viewing patient-specific information which is necessary to satisfy your clinical responsibilities.**
- **Accessing/viewing information on a "need to know" basis in order to provide and/or support qualitypatient care processes.**

Examples of legitimate, proper use:
*View your / your doctor's patients
*View patient demographics on your / your doctor's new admissions or consults
*Verify admission & discharge dates
*Verify insurance information
*Obtain precertification numbers
*Verify addresses
*Check patient status (inpatient vs. observation)
*Check for referring physicians (consults)

INAPPROPRIATE ACCESS:

- **Viewing your OWN record**
- Viewing your friend's or neighbor's information when you/your supervising provider is not providing patient care
- **Viewing a relative's information…. INCLUDING SPOUSE and CHILDREN without a release ofinformation**
- Looking at an employee's information…even if he/she requests you to do so…if you/your supervising provider is not providing care
- **Letting someone else use your password**
- Viewing the electronic health record of any patient for whom you / your supervising provider is not providing care

NOTE: If you would like copies of your medical records (or your minor-age child's records), please call or visit the Health Information Management - Medical Records Department or sign up for the patient portal.

NOTICE OF PARTICIPATION ELECTRONIC SIGNATURE

IF THIS SECTION DOES NOT APPLY TO YOUR ROLE PLEASE LEAVE BLANK

This is to notify you that I will participate in the use of electronic signature to authenticate entries any place in the medical record where a physician or appropriate hospital staff signature is required. Other types of documentation.

I agree that my PIN or pass code chosen by me is to remain confidential and it is my electronic or computer-generated signature to be used only by me. I certify that I will not disclose the confidential code (PIN or pass code) to another person for their use. I understand that the Medical Executive Committee will be notified if I misuse electronic signature by allowing another person or persons to use my confidential code (PIN or pass code).

Requester Signature _____ Date _____

First Name

Last Name

Dept Facility/Location

Email Address

Return completed form to the Medical Staff Services Department Email credentialing@ouhealth.com