OU Medical System
OU Medical Center | The Children's Hospital | OU Medical Center Edmond

MEDITECH ACCESS REQUEST
PHYSICIAN OFFICE STAFF

Please complete ALL required fields as indicated with an *

MUST submit 2 weeks prior to start date

Incomplete agreements WILL NOT be accepted or processed and could result in delayed access!

***FULL Name** (Please Print):_____**Initials:** ___ ___ ___ ____ ____

LAST Name **FIRST Name** **Middle Initial**

If you only have 2 initials, use X as middle initial

==========

For research study purposes, will you have patient contact within the Hospital? **Circle one:** **Yes** **No**

If yes, please contact OUMS Med Staffing Office at 271-3741 to receive a research credentialing packet and the required Hospital badge **BEFORE** faxing your agreements.

***DOB** _____/_____/_____ ***Personal Phone #: (_____) - _____ - _____**

***Home Address** _____

***City** _____ **State**_____ **Zip:**_____

***E-Mail** _____

***Department** _____ **Department Phone#**_____ **Ext.**_____

***Job Role/Title:**_____ **Supervisor?**____

***User needs same access as:**_____

(name of employee or co-worker who has current access)

Please list FIRST & LAST names of physicians whose patients' records you need to access:

_____

_____

***If you change departments, you will need to re-sign the Meditech Access Request and Information Security Agreement to retain access.**

I have read the examples and understand Appropriate Access of patient information. I agree to look ONLY at patient information on a need-to-know basis to do my job. I understand that **ACCESSING MY OWN or A FAMILY MEMBER'S or CO-WORKER'S Meditech record is inappropriate access.** I will not let someone else use my Meditech ID and password. I will log off /exit Meditech when I leave the computer.

I will receive/have received Meditech training on the portions of the system for which I have received access.

***Signature:** _____ Trained by: _____

****

****MUST be completed by Physician****

By my signature below, I authorize this employee's Meditech access to my patients' records and accept responsibility for access to the physicians' patients listed above and those I add to my patient list. Physicians listed above are in my cross-cover and Provider Group. **I understand that I am responsible to notify the IS Physicians Support Analyst at OU MEDICAL CENTER when office staff leave my employment.**

Physician Signature _____ **Date:**_____

Physician Name Printed _____ **Date:**_____

Fax Completed forms to 271-2741 or email to oumc.physiciansupport@oumedicine.com

Vendor Confidentiality and Security Agreement

Note: this form to be used for individual vendor representatives.

I understand that the OU Medicine, Inc. and its affiliated facilities and entities (collectively, "OUMS" 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 assignment at 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 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 privileges, and/or termination of authorization to work within the Company facilities or with Company data.

Protecting Confidential Information

4. 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.
5. 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.
6. 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).
7. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
8. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards (provided upon request).

Following Appropriate Access

9. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
10. I will not attempt to bypass Company security controls.
11. I will only access software systems to review Company information when I have a business need to know, as well as any necessary consent. By accessing 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.

Using Mobile Devices, Portable Devices and Removable Media

12. I will not copy or store Confidential Information on mobile devices, portable devices, or removable media such as laptops, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job assignment. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards (provided upon request).

13. I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes Company data (*e.g.*, Company email) may contain Confidential Information and as a result, must be protected as required by Company Information Security Standards (provided upon request).

Doing My Part – Personal Security

14. 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.
15. 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.
16. I will never:
    a. Disclose passwords, PINs, or access codes.
    b. Allow another individual to use my digital identity (e.g., 3-4 User 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.
17. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
18. I will immediately notify the OUMS Information Security Official, OUMS Director of Information Technology, or OUMS 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

19. 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.
20. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
21. 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.

Vendor Signature		Date
Vendor Printed Name		

PLEASE READ BUT DO NOT FAX THIS PAGE!

OU Medical System
OU Medical Center | The Children's Hospital | OU Medical Center Edmond

APPROPRIATE ACCESS
System s User's Guide

CONFIDENTIALITY...

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

APPROPRIATE ACCESS:

Viewing patient-specific information which is necessary to perform your professional job responsibilities

Accessing/viewing information on a "need to know" basis in order to provide and/or support quality patient care processes.

*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 physician's consults

INAPPROPRIATE ACCESS:

Viewing your OWN record

Viewing your friend's or neighbor's information when you/your supervising physician is not providing patient care

Viewing a relative's information….INCLUDING SPOUSE and CHILDREN without a release of information

Looking at an employee's information…even if he/she requests you to do so…if you/your supervising physician is not providing care

Letting someone else use your password

Viewing the electronic medical record of any patient for whom you / your supervising physician 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.

PLEASE READ BUT DO NOT FAX THIS PAGE!

OU Medical System

OU Medical Center | The Children's Hospital | OU Medical Center Edmond

Please FAX to 405-271-2741 or email to oumc.physiciansupport@oumedicine.com

1. **Confidentiality and Security Agreement**
   - ***Sign at the bottom.**

2. **Meditech Access Request**
   - ***Complete the top section.**
   - ***Sign that you understand Appropriate Access.**
   - ***Sign that you have had training or will be trained by another person with whom you are working.**
   - ***Physician Office Staff must have a physician signature at the bottom of the Request.**

OUMS Physician Support Helpdesk

OU MEDICAL SYSTEM

Email: oumc.physiciansupport@oumedicine.com
Fax: 405-271-2741
Phone: 405-271-8660 choose Option 1, then Option