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

MEDITECH ACCESS REQUEST

Fellows, Residents, Interns

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.

==========

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

***Home Address** _____

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

***E-Mail** _____

==========

New request _____ Change from Student to Resident _____ Resident to Fellow_____

==========

***Will you be providing care or consulting on NICU or Women's Services patients? Yes / No**

Current Medical Department _____ Current Attending Phys or Chief Resident _____

(Please circle level.) Resident Fellow MD DO DO-1st yr

***Date that I plan to BEGIN** _____ ***LEAVE** _____ OUMS

I am here for a rotation from St. Anthony's___Griffin Memorial___Integris___ Other _____

==========

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 I may ONLY look at a family member's record following a signed Release of Information in the paper chart. I will log off /exit Meditech when I leave the terminal/computer. I will not let anyone else use my Meditech ID or password.

I have received Meditech training or I will receive training from a peer or Physician Support Coordinator on the portions of the system for which I receive access.

Signature _____**Date:**_____

==========

FAX to OUMS Physician Support @ (405) 271-2741 or email to
oumc.physiciansupport@oumedicine.com

Please call if you or another person would like Meditech assistance or training.
OUMS Information Systems Physician Support 405-271-8660, Option 1, then 2

Provider Confidentiality and Security Agreement

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

I understand that 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 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 OUMS medical staff, I may no longer use OUMS'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 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 OUMS 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 m**

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).**
    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., 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.**
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, 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

24. **I agree to notify the OUMS 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.

Provider Signature		Date
Provider Printed Name		

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

APPROPRIATE ACCESS
Systems User's Guide

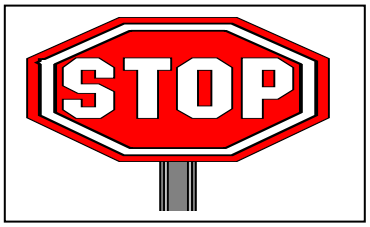
CONFIDENTIALITY...

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.

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.**

OUMS Information Systems
Physician Support

Email: **oumc.physiciansupport@oumedicine.com**
Fax: **(405) 271-2741**
Phone: **(405) 271-8660, option 1, then 2**

Appendix A
OU MEDICAL CENTER
NOTICE OF PARTICIPATION ELECTRONIC SIGNATURE

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).

Signature: _____ Date: _____

Print Name: _____

Medical/Hospital Department: _____

E-Mail address: _____

Electronic Signature PIN

Must be 4 numbers.

The PIN that I would like to use is: _____

Please print your PIN clearly!

Your PIN…..remains the same unless you ask for it to be changed.

Print Name: _____

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

OU MEDICAL CENTER
Hospital Policy and Procedure Manual

Subject: Electronic Signature

Section: 17-09 **Page:** 1 of 3

Origination Date: 4/2001 **Revision Date:** 4/2005, 6/2008 5/2010

Coverage: Physicians and Appropriate Hospital Staff

Policy: Pursuant to Oklahoma State Statute regarding the use of electronic signature, OU MEDICAL CENTER has adopted the following policy:
Electronic or computer-generated signature of physicians and appropriate hospital staff are acceptable as authentication and may be used any place in the medical record where a physician or appropriate hospital staff signature is required, provided the signature is generated by a confidential code that only the user possesses and the following safeguards are adhered to:

- The physician or appropriate hospital staff must have a signed Notice of Participation statement on file within or at a location designated by the Medical Staff Services Department.
    - The physician/appropriate hospital staff will use electronic or computer-generated signatures to authenticate his or her entries in the medical record.
    - The signature will be generated by a confidential code which only the physician/appropriate hospital staff possesses.
    - No person other than the physician/appropriate hospital staff will be permitted to use the electronic or computer-generated signature.
- The physician's/appropriate hospital staff's use of an electronic or computer-generated signature is approved by the hospital's designee, the Medical Record Committee by acceptance of the electronic signature.
- The electronic signature must be the full, legal name and professional title of the physician/appropriate hospital staff.

Prior to entering the confidential code (PIN or pass code), the participating physician/appropriate hospital staff must personally review, edit and verify the place in the medical record where the physician or appropriate hospital staff signature is required and will be used as authentication.

System-specific standards and procedures for using electronic signature may vary from system to system. Department directors who administer systems which permit the use of electronic signature must establish and maintain system-specific procedures for managing the issuance of confidential signature codes and their use.

Procedure:

Responsible Party:	**Action:**
Physicians and Appropriate Hospital Staff	1. Participating physicians and appropriate hospital staff must sign a Notice of Participation Statement. 2. Participating physicians and appropriate hospital staff will choose a confidential code (PIN or passcode) which is their

Responsible Party:	Action:
	electronic or computer-generated signature. They must agree that they will not disclose the confidential code to another person for their use. 3. Prior to entering the confidential code (PIN or pass code), the participating physician/appropriate hospital staff must personally review, edit and verify the place in the medical record where the physician or appropriate hospital staff signature is required and will be used as authentication. Once an electronic or computer-generated signature is used to authenticate a record, the record cannot be changed. However, an addendum can be attached to the original record.
Information Systems or Department Director	1. Directors of departments who administer systems that provide for electronic signature must establish and maintain system-specific procedures for managing the issuance of confidential signature codes and their use. The procedures must meet the OU Medical Center Electronic Signature policy and provide for the following: 2. Assures an approved Notice of Participation statement is on file prior to issuing a confidential code (PIN or pass code). 3. System administrator configures physician/appropriate hospital staff confidential code (PIN or pass code) and provides physician/appropriate hospital staff education for use of electronic signature. 4. Provides for an audit of electronic signature use and addresses any misuse of confidential code (PIN or pass code). 5. Maintains a listing of all participating physicians/appropriate hospital staff. Maintains at a designated location or forwards to Medical Staff Services Department the original or a copy of the Notice of Participation statement. 6. Terminates physician system access which terminates the confidential code (PIN or pass code) when a physician is no longer credentialed, and terminates appropriate hospital staff access which terminates the confidential code (PIN or pass code) when hospital staff terminate employment.
Medical Staff Services Department	Maintains or designates where copies or originals of the Notice of Participation statements will be stored.
Medical Record Committee	Approves physician/appropriate hospital staff use of electronic or computer-generated signature by acceptance of the electronic signature.
Health Information Management	Provides physician education and procedural implementation for medical record completion.

See also Appropriate Access Policy and Procedures See also Confidentiality Policy and Procedures
See also IS and HIM Department specific Policies and Procedures

Supersedes: OUMC Policy 19-09, Electronic Signature, 6/2008

Approved Medical Records Committee: 7/2/2003
Approved Policy and Procedure Committee:
5/13/2010 Approved Medical Executive
Committee: N/A
Approved Board of Trustees: N/A

IMAGING NETWORK ACCESS REQUEST

*** ***PLEASE PRINT*** ***

Name: _____
LAST FIRST MIDDLE INITIAL

Last 4 digits of SSN: _____ MEDITECH USER ID: _____
DO NOT ENTER YOUR MEDITECH PASSWORD!!!

MEDICAL DEPARTMENT/COLLEGE : _____ PHONE #: _____

OFFICE LOCATION/SUITE #: _____

STATUS (Check one): ❑ Faculty ❑ Fellow ❑ Resident ❑ Intern ❑ Medical Student
❑ PA ❑ Nurse ❑ Rad Tech ❑ Staff/Other _____

E-Mail Address: _____

- ***I have read and understand the attached OUMC APPROPRIATE ACCESS policy regarding patient information.***
- ***I agree to look ONLY at patient imaging information on a need-to-know basis for the performance of my duties.***
- ***I will LOG OFF the imaging workstation when I leave.***

_____ _____
SIGNATURE DATE

Please fax the completed form to (405) 271-1153

FOR INFORMATION SYSTEMS USE ONLY

DATE RECEIVED: _____ _____
INITIAL

TRAINED? ❑YES ❑NO DATE RECEIVED: _____ TRAINER: _____

APPROVED? ❑YES ❑NO REASON IF NO: _____

DATE ACCESS GRANTED: _____ _____
INITIAL

DATE USER NOTIFIED: _____ _____
INITIAL

HOW NOTIFIED: ❑ E-Mail ❑ MOX ❑ Phone ❑ In Person ❑ Other _____

Form edited 09/08/11

Form created 7/15/04