

HEALTHCARE SYSTEMS AND TECHNOLOGIES CLINICAL SYSTEMS

Electronic Medical Records Subscription Access Request Form

IMPORTANT INFORMATION (PLEASE READ)

Training Requirements: All users are required to complete online training OR online and classroom training (depending on job role) before submitting this form. Please **PRINT** legibly and complete all fields.

NOTE: All individuals requesting Electronic Medical Record access must complete UH approved HIPAA and Compliance training programs.

- **Non-UH Individuals:** Requires a guest portal access account in order to register for the Centricity/Logician, Epic, MUSE, and PACS online courses. Speak to your sponsor.
- **Research Individuals:** Contact the Medical Informatics Committee at 973-972-1800 for the required forms for approval.
- **CENTRICITY/LOGICIAN, EPIC, MUSE, and PACS TRAINING INFORMATION:** Online training for Centricity/Logician, Epic, MUSE, and PACS found in UH Moodle.
- **To Receive your Centricity/Logician, EPIC, MUSE, and PACS IDs:** Upon successful completion of Centricity/Logician, EPIC, MUSE, and PACS training via Moodle and if required in-class training bring forms to **ADMC Building 10, Room 1005** between 8AM-4PM. Mon-Fri.

A - EMPLOYEE INFORMATION

- Reason for Application: (May choose more than one.) **NOTE: Incomplete forms and/or absence of supporting documentation of training will delay the processing of this request.**
 - Application:** EPIC Centricity/Logician MUSE PACS Other: _____
 - New User** **Current User:** Modify Account (User ID): _____
- Last Name: _____ First Name: _____ M.I.: _____
- Contact Number: _____ Department/Unit: _____ UPA (Faculty Practice)
- Employee ID (A#) : (**User authentication to meet HIPAA regulations**): _____ RUID (i.e. CORE ID) _____
- Title (check one): MD Community MD DO DMD DDS APN PA RN CRNA Anesthesiologist Fellow Nursing Assistant
 Respiratory Therapist Social Worker Case Manager Nutritionist Dietary Pharmacist Pharmacy Tech Staff RN Staff LPN
Faculty/Students: You must provide a Start/End Date. You will not be activated without this information: Start Date _____ End Date _____
Faculty/Instructors: Are you UH Staff?: ___Yes ___No: Medical Student Nurse Student Pharmacy Student PA Student SRNA
 Resident - Year _____ Program: _____ Rotator Resident OTHER (Check Job Role from Section B)
- Auto Sign Labs/Images in Centricity/Logician?
 - Yes (Disclaimer: By authorizing the system to Auto Sign Lab/Images, you are still considered responsible for any Labs/Images received in the system with your name as the ordering provider and expected to follow up any abnormal result thru other means of Patient Care.)
 - No (Disclaimer: You will be responsible to sign any Lab/Images received in the system with your name as the Ordering Provider)

B - JOB ROLES (Select only if #5 above does not apply)

All Applications - Clinical

- Central Supply Departure Clerk Medical Technician Nurse Manager Office Staff OR Scheduler Unit/Ward Clerk LAB Releaser
 RAD Releaser EKG Releaser Vascular Releaser OTHER: _____

Epic - Registration

- Admitting Clerk Admitting Manager Information Desk Inquiry Only Outpatient Clerk DOC Outpatient Clerk DOC w OpTime Outpatient Mgr DOC
 Outpatient Nurse DOC Outpatient Registrar DOC Patient Flow PAR Patient Flow Manager Medical Records _____ (indicate Role, i.e. coder, ptmerger,)

Epic - Scheduling/Registration (Cadence) : LEVEL 1 LEVEL 2

- Ambulatory Care Tech Non-Certified Ambulatory Care Tech Certified Inquiry Scheduler Template Manager

C - SIGNATURES

Employee Signature: _____ Date: _____
Class/Trainer: _____ Training Date: _____ (if classroom training is required)
Manager Signature: _____ Manager Print Name: _____ Date: _____ Phone#: _____

FOR HST USE ONLY:

Date received @ HST: ___/___/___ HST Management Authorization: _____ Date: ___/___/___
Epic User Type : _____ Epic User Template: _____ HST Analyst: _____ Date: ___/___/___
Date ID Created for : _____ by _____ Given to User: _____ User ID assigned: _____
(application) (date) (date)

Instruct user of requirement to present this to HST upon completion of training for all systems requested. HST to make copy of this completed form for the user. This form will be used to create ID's for Epic, Centricity/Logician, MUSE, and PACS.



Information Security and Confidentiality Agreement

SCOPE OF AGREEMENT:

Universal Hospital (“UH”) is committed to maintaining high standards of data security. Every User, as defined below, is responsible for preserving and protecting the confidentiality of electronic data. UH reserves the right to monitor and/or inspect all UH systems to ensure that Confidential Information, as defined below, is protected at all times. The terms of use of such UH systems are set forth below.

DEFINITIONS:

Agreement means this UH Information Security and Confidentiality Agreement.

Confidential Information means confidential information that is created, maintained, transmitted or received by UH and includes, but is not limited to, PHI, other patient information, information relating to any employee, volunteer, trainee, contractor, physician, medical, financial and other business-related or company private information in any form (e.g., electronic, verbal, imaged or written).

Protected Health Information (“PHI”) means individually identifiable health information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. PHI can be oral, written, electronic, or recorded in any other form.

User means a person or entity with authorized access to any UH network and/or other information systems, including computer systems.

I AGREE TO THE FOLLOWING:

1. I understand it is my personal responsibility to read, understand and comply with all applicable UH policies and procedures. I understand that these policies provide important information about protection of PHI and the acceptable use of information systems, protection from malicious software, mobile device usage, data encryption, and other important information.
2. I agree not to disclose any Confidential Information obtained by accessing the UH network and/or other information systems, including computer systems or otherwise, to any unauthorized party.
3. I agree not to access, destroy, copy or use any Confidential Information unless I am authorized to do so.
4. I agree to access the UH network and/or other information systems, including computer systems, only for purposes related to the scope of the access granted to me and only in furtherance of the performance of my job function.
5. I agree to log-off and secure my workstation when unattended.
6. I understand that UH regularly audits access to information systems and the data contained in these systems and can revoke my access at any time. I agree to cooperate with UH regarding these audits or other inspections of data and equipment, including UH inquiries that arise as a result of such audits.
7. I agree that I will not share or disclose User IDs, passwords or other methods that allow access to UH network and/or other information systems, including computer systems, to anyone, at any time, nor will I share my account(s). I also agree to store all UH company-related data onto the system servers rather than on hard drives of individual workstations, personal computers or other devices.
8. I agree to contact my supervisor (or for non-employees, the applicable UH Department Director or UH business contact) and the UH Information Security Officer and change my password immediately if I have knowledge that any password is inappropriately revealed or any inappropriate data access or access to Confidential Information has occurred.
9. I understand the definition of Confidential Information set forth above.

10. I agree that I will not install, download, transmit or use software that is not licensed by UH (or that is otherwise unlawful to use) on any UH information systems, equipment, devices or networks. I understand that unauthorized software may pose security risks and will be removed by UH.
11. I agree to report any and all activity that is contrary to this Agreement or UH policies to my supervisor, Department Director, IS Security Officer or Privacy Officer.
12. I understand that to the extent I am an employee of UH, this form will be included in my employee file at UH and that failure to comply with this Agreement and UH policies may result in formal disciplinary action, up to and including termination. I understand that to the extent I am a contractor, failure to comply with this Agreement and UH policies may result in revocation of access and the termination of any agreements or relationships with UH.
13. I understand that all information and/or data transmitted by or through or stored on any UH device, or system maintained on UH's behalf by a vendor or other individual or entity, will be accessible by UH and considered the property of UH, subject to applicable law. I understand this includes, without limitation, any personal, non-work related information. I do not have any expectation of privacy with regard to personal, non-work related information on any UH network and/or other information systems, including computer systems, and understand that UH has no obligation to maintain the privacy and security of the information. I understand that UH reserves the right to monitor and/or inspect all systems that store or transmit UH data, the data stored therein, as well as all documents created by or on behalf of UH.
14. I agree to comply with UH requirements to encrypt electronic Confidential Information in accordance with UH policies, including the requirement that encryption software be installed on all UH-owned laptop computers and that all emails containing Confidential information transmitted over an electronic network outside of UH be encrypted, as described in the UH security policies.
15. I agree that all devices used by me that are connected to a UH network and/or other information systems, including computer systems, whether owned by me or not, must be continually running approved and updated anti-virus software. I agree to adhere to warnings about computer viruses and perform virus can updates as directed.
16. I understand that UH equipment should only be used for the purpose of performing my job or services, except on occasion for minimum personal use as set forth in the Acceptable Use policy, Issue No. IST-PL-001. I understand that in no event shall I transmit or display abusive, discriminatory, harassing, inflammatory, profane, pornographic, offensive language or other such materials over or on any UH network or system.
17. I will follow the requirements for Users described in all UH policies, including but not limited to the UH Information Systems Acceptable Use Policy. The UH Information Security and Privacy Policies are available through the UH Office of Ethics & Compliance, the UH Information Security Office and the MCN Policy Manager.
18. I understand that my obligations hereunder are ongoing and require me to review the policies for updated materials, as well as participate in additional training as policies are updated and new technology is added.

By signing this Agreement, I understand and agree to abide by the conditions listed above.

Signature

Print Name

Date

Employer

Title/Position

Department

This Agreement must be signed and on file for each User before access is provided to such User.