

OACIS Security Agreement

PURPOSE:

To protect the confidentiality, integrity and security of patient information in the electronic medical record (EMR) accessed via OACIS and Citrix Webapps, through the use of a unique and private user identification code/username and password.

POLICY:

Healthcare information can be accessed by authorized persons to support patient care, peer review, quality improvement, risk management, reimbursement claims, clinical research, education and other legitimate requests. Any unauthorized use or disclosure of patient information is strictly prohibited. Access to various categories of patient information is based on need and defined by job title and function. OCIO-IS reserves the right to refuse access to the electronic medical record until proof of authorization is obtained.

Authorized persons will be issued a unique user identification code and password. The username provides appropriate access levels and serves as an electronic mechanism for tracking/auditing access and entries to the EMR. **THESE ARE PRIVATE IDENTIFICATION CODES AND ARE NOT TO BE SHARED OR MADE PUBLIC.** Users must sign off or exit OACIS before leaving the workstation. If a user has any reason to believe that his sign-on code has been shared or compromised, he must immediately change his/her OACIS password and report the incident to his/her supervisor. Upon termination of employment with MUSC or its affiliates, the user's sign-on code will become inactive.

Failure to abide by the above policy can result in disciplinary actions including the discontinuation of computer privileges, job termination and criminal charges. (See Policy C-27 of the MUSC Medical Center Policy Manual)

PROCEDURE:

- Obtain a Security Agreement** from a preceptor, unit educator, Information Technology Coordinator, or other designated department coordinator. Security Agreements can be printed from the OCIO-IS web page (<http://www.musc.edu/infoservices/forms>) or can be obtained by calling the OCIO-IS Support Desk at 792-9700.
- Complete all fields of the OACIS Security Agreement, then sign and date the form.** Failure to do so can result in a significant delay in processing your request. (Additional copies of this agreement can be found at the following URL: <http://www.musc.edu/infoservices/forms>. You may also call the OCIO-IS Support Desk at 792-9700).
- Return the completed form to OCIO-IS.** Forms may be faxed to **792-8315**, or sent via campus mail to OCIO-IS, Harborview Office Towers, Suite 210, PO Box 250801.
- Present ID and pick up new sign-on code.** Employees, faculty, house-staff, and students must present their official MUSC employee identification badge to receive their code. Non-MUSC authorized users must present a secure form of personal identification (driver's license, passport etc) when receiving an OACIS access code. (To determine if special conditions exist for delivery of codes to locations greater than 1 hour travel time from MUSC or for large off-site groups, please call the OCIO-IS Support Desk 792-9700)

**New codes should be available 48 hours after your request is faxed, or 1 week after request if sent via campus mail.
 PICK UP LOCATION (24 HOURS, 7 DAYS A WEEK) Medical Records, Main Hospital, Room 269**

- Please direct all questions or problems, i.e., forgotten password, to the OCIO-IS Support Desk, 792-9700.**

FULL Name: _____ (PLEASE PRINT) Credentials: _____ (RN, MD, CA, PCT, RT, etc.)

DOB: _____ Phone: _____ Job Title: _____

NetID: _____ Email Alias: _____

Department/Division: _____ Unit: _____

Department Chair/Supervisor: _____ Phone: _____

ANSWER ALL THREE QUESTIONS:

- Mother's Maiden Name? _____
- Father's Middle Name? *(put first name if no middle name)* _____
- Town where you were born? _____

Your signature below indicates that you have read and agree to comply with the above policy and procedure.

Signature: _____ **Date:** _____

For Office Use Only	OACIS LoginID: _____	UID: _____	Temp Password: _____
	Date Trained: _____	Analyst's initials: _____	Date Completed: _____