MEDICAL UNIVERSITY OF SOUTH CAROLINA – OCIO-Information Services

eCareNet Viewer: NEW ACCOUNT for NON-MUSC Associate

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:

Health care 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-Information Services (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 MUSC Sponsor.

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

PROCEDURE:

1. **Obtain a Security Agreement** from an OACIS Team Representative.

2. **Completely read, fill out and sign the security agreement**. Failure to fill out this form in its entirety will result in your request being denied.

3. **Return the completed form to OCIO-IS.** The form can be faxed to 843-792-8315 , or sent via campus mail to OCIO-IS, Harborview Office Towers, Suite 210, PO Box 250801.

4. **Receipt of OACIS Login Codes:** Non-MUSC authorized users must read, fill out and sign the OACIS – Citrix Non-MUSC Associate New Account form and the MUSC C-27 Policy and fax them to OCIO-IS at 843-792-8315 . **You will receive an email within two business days with your username and password information.**

5. **Forgot your password?** Call the OCIO-IS Support Desk to report this.

6. **Direct all questions or problems to the OCIO-IS Support Desk, 843-792-9700.**

FULL Name: _____

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

NPI # (NP, PA and MD only)_____

Last 4 digits of your social security #:_____

DOB: _____ Phone: _____ Job Title: _____

NetID: _____ MUSC Email address: _____

Department/Division: _____ Unit: _____

Department Chair/Supervisor: _____ Phone: _____

ANSWER ALL THREE QUESTIONS:

1. Mother's Maiden Name? _____
2. Father's Middle Name? *(put first name if no middle name)*_____
3. 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:** _____

Revised 01/05/09

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

MEDICAL UNIVERSITY OF SOUTH CAROLINA
MUSC MEDICAL CENTER POLICY MANUAL
Policy C-27

SUBJECT: CONFIDENTIALITY OF PATIENT INFORMATION AND MEDICAL RECORD SECURITY

PURPOSE:

To ensure that patient information is protected from unauthorized use and to establish standards regarding the use of patient information for the Medical University of South Carolina and its employees and affiliates, consumers, students, external collaborators, auditors, contractors and vendors.

POLICY:

Medical University of South Carolina (MUSC) has a duty to treat patients with respect for their personal dignity and right to privacy, and to protect the confidentiality of information concerning their care.

Health care information will be released to authorized persons to support patient care, peer review, quality improvement, risk management, reimbursement claims, clinical research, education and other legitimate requests. Access to verbal, written or electronic patient information is provided for authorized purposes only. Any unauthorized use or disclosure of patient information is strictly prohibited.

MUSC adheres to all state and federal laws as well as all other applicable regulatory requirements in recognition that medical records are confidential and shall not be released or disclosed to any unauthorized persons.

Medical records are acknowledged as legal and confidential information and must be stored, secured, and processed according to established MUSC policy.

Recognizing MUSC owns the storage media, but the patient owns the information, patient information will be released upon proper authorization from the patient or his/her legal representative and as required by state or federal statute, subpoena, court order. Access to information does not imply jurisdiction; therefore patient information is to be released only by those individuals who have the authority to release. Fees may be charged for reproductions.

Documents which may be stored but are not to be released are: birth certificates, death certificates and requests/authorizations.

Paper medical records must remain on institutional premises to be available for patient care at all times. Removal of paper records from the institutional premises is strictly prohibited except by court order or subpoena. All Medical University employees, faculty , housestaff and students who violate this policy will be subject to disciplinary action.

Disposal of patient-identifiable information, regardless of the type of media such as paper records, video, audio recordings, computer disks, plastic cards, etc., must be done in such a fashion that the confidentiality of such records is protected (e.g., by means of shredding, demagnetizing, etc.).

Employees, faculty, housestaff and students must present their official MUSC employee identification (ID) badges at the time a request to review or retrieve a paper record is made. (See A-7 Identification Cards Policy). Similarly, employees, faculty, housestaff and students must present their MUSC ID badges in person when receiving computer access codes to MUSC's electronic medical record system. Non-MUSC users must have an appropriate faculty sponsor who signs a form stating the particular non-MUSC user requires 'need to know' access. The non-MUSC user must also present a secure form of personal identification (i.e., driver's license, passport, etc.) as well as other identifying information (e.g., date of birth, mother's maiden name) when first receiving computer access codes to MUSC's electronic medical record system. On each 12-month anniversary thereafter, non-MUSC users must be 'renewed' in writing by the faculty sponsor and contacted verbally to identify themselves (e.g., telephone), as well as sign a new confidentiality agreement, otherwise access will be discontinued. Both MUSC and non-MUSC users (vendors, consultants, etc.) must read and sign a copy of the attached "Confidentiality Agreement" (Appendix A) prior to receiving access to the electronic medical record system.

KEY TERMS AND DEFINITIONS:

"Automated" refers to computerized or electronic mechanisms.

"Authorized Access" is access granted by direct patient/guardian/parental consent; conferred by statute or regulatory requirement; or granted on a "need to know" basis as documented by privileges granted, position description or contract with the facility.

"Administrative" health record items pertain to data that identify the patient, or financial, legal, or demographic facts unrelated to clinical care that are maintained for health care evaluation or support beyond the clinician-patient relationship. The patient's name and address, the name and address of the guarantor, or the name and address of legal next of kin would be examples of administrative items. Some items that appear to be administrative items are considered clinical, such as the association of admission type or location with certain sensitive illnesses (see "Clinical" care items below). Direct mailing lists potentially used for marketing or patient satisfaction surveys would be further examples of administrative usage. Revised 09/08

"Clinical" care items pertain to any data in the health record obtained through the direct clinician-patient relationship as a result of examination, testing, treatment, observation, or conversation, as well as identifiable items that have clinical implications, such as the association of admission type or location with certain sensitive illnesses. Diagnoses, test results, physical examination notes, progress notes, and consultation findings are examples of clinical care items.
"Confidentiality" pertains to the treatment of information that an individual has disclosed in a relationship of trust, and with the expectation that it will not be divulged without permission to others in ways that are inconsistent with the understanding of the original disclosure. Confidentiality includes the right to control how one's information will be handled or used.
"Guests" is defined as those contracted and affiliated entities that are authorized to gain access to patient information for the purposes of supporting automated systems, such as contractors or software vendors who are assisting MUSC in the implementation and troubleshooting of patient-related computer systems, or other approved collaborators to MUSC.
"Identified data" are data on a particular patient where the identity of the patient is known and is essential to accomplish the user's purpose. Use of the health record for the direct care of patients, for education, for certain forms of research, for the settlement of an insurance claim, or as evidence in a civil court are examples that fall into this category
"Legal Medical Record" for MUSC shall consist of all authenticated documentation, handwritten and/or electronically generated, created during the normal course of business, which relates to the care of an individual patient regardless of storage site or media.
"Non-Identified data " are data where the information itself, rather than the patient whom it describes, is the object of interest. Therefore, for "non-identifiable" purposes, the identity of the patient is not disclosed. Certain statistical, research, and educational projects typify such access.
"Privacy" can be defined in terms of having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. Privacy includes the right to determine what, if anything, will be known about oneself.

INFORMATION/BACKGROUND:

MUSC recognizes that consumers/patients retain their rights of privacy and confidentiality of personally identifiable information obtained from any source and used for any purpose. All information pertaining to a patient's identity, location, clinical history, or diagnosis and treatment is considered confidential.
MUSC recognizes that although the medical record is the property of MUSC, information in the record is acknowledged as belonging to the patient. Therefore it is the patient's right, or the right of their legally authorized representative, to authorize the release of the information to a third party. It is also recognized that patients or their legally authorized representative may access information in their medical record according to the procedures for release of information.
The fundamental responsibility of protecting access to and use of any health-related patient information rests with each person who has contact with patient information.

PROCEDURES:

1. Individuals Covered:

Users who access patient information should do so on a 'need to know' basis according to their job function. The following is a partial list of users of health-related information. Users requesting specific access for specific patients or groups of patients, must have signed an appropriate security and access contract for use of an automated patient information system (See Policy A-35, Managing Automated Data and Information). In addition, the following must sign a Confidentiality Agreement (Appendix A) and to be bound by this Confidentiality Policy:
A. Health care providers and health care team members, including faculty, house staff and students who train at MUSC, as well as non-MUSC consultants and referring providers who receive access to the electronic medical record system who are designated as being responsible for the care of a specific patient or group of patients, or ancillary personnel providing direct support for the care of a specific patient, group of patients, or a specific patient information function.
B. Supervisors of health care providers, or those held accountable for the clinical care provided for a patient or group of patients.
C. MUSC Legal Counsel, compliance, audit and risk management personnel, including internal and external bodies responsible for protecting the legal and regulatory interests of MUSC.
D. Authorized personnel conducting program monitoring, program evaluation, quality improvement, service reviews, data administration, billing, and data retrieval for authorized purposes.
E. Authorized personnel providing technical support and/or maintaining the integrity of automated systems at MUSC.
F. Transcriptionists and transcription services or other authorized consultants/vendors outside MUSC who have been contracted for transcription of patient records or other approved services. Revised 09/08

G. Persons authorized to do exempt or non-exempt research by approved research protocols (with adequate human subjects confidentiality statements when required, such as in Appendix A of the Institutional Review Board (IRB) application) to collect and analyze patient data for research purposes.
H. Guests of MUSC who require access to a computer system for the purposes of system review or support may have access to a training module of the system which does not contain real patient data. For guests who view real patient data, a non-disclosure statement must be signed.
I. Persons who are contracted by MUSC to warehouse, store or maintain patient records.

2. Forms of Information Subject to Confidentiality Policy:

A. Written Record - Paper documents relating to an individual's healthcare, whether handwritten or computer generated, are subject to this confidentiality policy. Paper research and clinical records held by an individual healthcare provider or in a particular department are all materials requiring protection from inadvertent disclosure under this confidentiality policy.
B. Audio/visual - Audio tapes, or products of dictation, whether digitally available or accessible by phone, are additional media falling under this policy. Also included are any photographs, video recordings or other visual images in which the patient is identified or potentially identifiable.
C. Spoken conversations - Spoken conversations concerning patient information, regardless of location, must be treated as confidential Patient information must never be discussed in public areas.
D. Automated - All identified or potentially identifiable patient information captured, stored or retrieved through automated systems must be treated as confidential.

3. Types of Information/Content:

The following categories should be used as guides when requesting the release of information from the Health Information Services (Medical Records) Department of the MUSC Medical Center or custodians of patient records:
A. Determine whether data needed are identified or non-identified data, and whether the data are needed for 1) administrative, 2) clinical, 3) educational or 4) research use. The legitimacy of the requestor and the stated use of the information must always be taken into account prior to granting release.
B. Determine who will give authorization for the release of the information, who will get the information, what the information will be used for, how long a time period does the authorization cover, what data items are to be released, and if the release covers a secondary authorization of the information.

4. Audit Trails:

An audit mechanism will be maintained for all persons requesting or accessing automated information. Monitoring of this audit information will be performed on a regular basis. Auditing will include random reviews of computerized patient access and the type of information reviewed.

5. Access to Administrative Patient Information (Identified):

Please see existing MUSC Medical Center policies on this topic including: C-3, Patient Confidentiality, Policy C-4, Confidentiality of Patient Location Information, Policy C-5, Also Known As (AKA), and Policy C-28 Release of Information From Medical Records.

6. Access to Aggregate Patient Information (Non-identified):

Access to aggregate patient information is provided to MUSC health care and support personnel for purposes of operations, 'need to know', job function, statistics, quality improvement, peer review, clinical research and education.
Written approval is otherwise needed from one of the following:
- Appropriate Attending Medical/Dental Staff practitioner
- Clinical Chief(s) of Service (or Deputy as designee)
- MUSC Institutional Review Board (IRB) for Human Subjects

Research-related requests for aggregate patient information contained in paper charts should be submitted to Medical Records on forms provided for this purpose. Such forms will indicate the reason/purpose the information for which is being requested as well as an acknowledgment by the requestor assuring confidentiality of the data. If the researcher intends to publish, present or otherwise disseminate the findings from the research, relevant protocols will be forwarded to the IRB to be reviewed in accordance with the standard approval process.
Research-related requests for non-identified aggregate patient information contained in the electronic data repository will be submitted by means of a suitable search engine or data-query tool, under the terms of an IRB-approved protocol. If the researcher intends to publish, present or otherwise disseminate the findings from such queries, relevant protocols will be forwarded to the IRB to be reviewed in accordance with the standard approval process. Prospective IRB review and approval must be obtained prior to obtaining any patient identifiers or data intended for publication.

VIOLATIONS/SANCTIONS: Revised 09/08

Violation of the confidentiality of patient information or a compromise to patient information system functionality is considered to be a serious offense and subject to disciplinary and/or legal action up to and including non-matriculation or termination in accordance with MUSC Human Resources Management Policy #45: Disciplinary Action.

Any serious and deliberate breach of patient confidentiality committed for personal gain, or a violation which results in damage to a patient, employee, the integrity of the data system, or the university, should always be treated as a serious violation, and legal action may also be a consideration.

Date Originated: 1/80 Legal Review Date: 2/97, 10/00
Date Reviewed: 10/95, 1/97, 5/97, 6/00 Date Effective: 3/97, 10/00
Date Revised: 10/95, 5/97, 8/00 Revised 09/08

APPENDIX A
CONFIDENTIALITY AGREEMENT
Medical University of South Carolina

IMPORTANT: This agreement applies to all individuals who receive access to MUSC's clinical computing resources, whether you are an employee of MUSC or not. Please read all sections of this Agreement, in addition to MUSC policy C-27, Confidentiality of Patient Information and Medical Record Security. If you have any questions, please ask them before signing. You will receive a copy of this Agreement, and the original will remain on file at MUSC.

CONFIDENTIAL INFORMATION AGREEMENT

I recognize that the services provided by MUSC for its patients/clients are private and confidential; that to enable MUSC to perform those services, patients furnish information with the understanding that it will be kept confidential and used only by authorized persons as necessary in providing these services; that the good will of MUSC depends upon keeping services and information confidential; that certain legal obligations attach to this information and that by reason of my duties or in the course of my employment I may receive or have access to verbal, written, visual or electronic/automated information concerning patients and services performed by MUSC even though I might not furnish the services provided for those patients.

I hereby agree that, except as a part of my job responsibilities or as directed by MUSC or by legal process, I will not disclose any such services or information. Furthermore, I will not permit any person to inappropriately examine or make copies of any reports or other documents, or any information to which I have access, that concerns in any way the patients of MUSC. I also agree that I will not access or review patient information for any reason not related to the provision of clinical care or other authorized purposes such as research, education, quality assurance, billing or utilization review.

I will not at any time reveal to anyone my confidential access codes to MUSC's information systems, and I will take all reasonable measures to prevent the disclosure of my access codes to anyone. I also understand that MUSC may, at any time, monitor and audit my use of the electronic/automated record and information systems.

I understand that this agreement is in effect both during and after my involvement in any activity related to the care and treatment of patients of MUSC.

I have read, understand, and agree with this Confidentiality Agreement as well as the MUSC Medical Center Policy on Confidentiality of Patient Information and Medical Record Security (C-27). I recognize that unauthorized disclosure or access of information by me may violate state and federal laws and cause irreparable injury to MUSC or harm to the patient, and may result in disciplinary and/or legal action being taken against me.

Signature	**Date**
Printed Name	
Sponsor Signature	**Date**