AHMC Anaheim Regional Medical Center

Security Policy/Systems Access Request Form

PLEASE READ AND UNDERSTAND

PURPOSE: To provide a uniform and consistent approach to acquisition and handling of computerized confidential information acquired during employment, or student rotation at Anaheim Regional Medical Center and associated sites.

POLICY: It is the policy of Anaheim Regional Medical Center that all individuals given access to ARMC computer assets sign an agreement that outlines the responsibility of the individual in dealing with confidential information. Responsibility for the maintenance of IDs and passwords will rest with the Security Officer assigned by the Director of the Information Systems Department.

PROCEDURE:

A. **REGISTRY STAFF**: Must complete and sign a Systems Access Request Form prior to being issued a username/password. A Copy of the form should be kept in the Nursing Administration where Registry Staff report for assignments and are issued passwords.

B. **STUDENTS**: Students must complete and sign a Systems Access Request form prior to the start of their rotations. For Nursing Students: Signed copies should be forwarded to Education Department, NO LATER THAN 2 BUSINESS DAYS (MON-FRI) PRIOR TO THE START OF THE CLINICAL ROTATION. For NON-NURSING STUDENTS: Signed forms must be forwarded to the Department Director or their Designee a MINIMUM OF 2 BUSINESS DAYS (MON-FRI) PRIOR TO NEED FOR COMPUTER ACCESS.

C. **TERMINATIONS-REGISTRY STAFF & NON-NURSING STUDENT ACCESS**: Will be terminated by the Issuing Department within the time guidelines agreed upon between the Department Director and the Information Systems Director. FOR NON-NURSING STUDENTS: Access will be terminated within one business day (Mon-Fri) of the known end of the rotation, or if previously unknown upon notification of the end of the individual students rotations. **NURSING INSTRUCTORS ARE RESPONSIBLE TO NOTIFY THE EDUCATION DEPARTMENT OF ANY STUDENTS TERMINATING THEIR ROTATION EARLIER THAN DEFINED AT THE START OF THE ROTATION.**

D. **CHANGES**: At the time job functions change that would affect level requirements, the Information Systems Department Director should be notified by a new Access Request Form.

E. **TEMPORARY EMPLOYEES/PROJECTS**: A temporary SIGN-ON and PASSWORD will be assigned for Temporary Personnel Projects. At the conclusion of the assignment, it is the responsibility of the Department Director to notify the Information Systems Director, either by Access Request Form or email, that the SIGN-ON/PASSWORD is no longer required.

ENFORCEMENT: Anaheim Regional Medical Center maintains that all information whether related to employment or medical treatment be kept confidential in compliance with HIPAA standards and not be disclosed without the proper authority. In order to provide for discrete use of the computer systems, it is expected that an individual's sign-on and password be kept confidential and not shared with other employees, students, patients, vendors, etc. Breach of confidentiality and/or proprietary information caused by violations of the policy regarding Sign-Ons may result in the following actions: The individual will be provided with a written warning and/or have disciplinary action taken up to and including termination for failure to comply with the Policies and Procedures of Anaheim Regional Medical Center.

PASSWORD EXPIRATION: We recognize over time it is possible that another person will gain access to your sign-on and/or password. To ensure that data is kept confidential, individuals will be required to change passwords as prompted. This will occur at varying times during the year for each user. If a user suspects that someone has gained access to their sign-on or password they should change their password immediately or contact the IS Department for assistance.

LICENSE AND APPLICATION STANDARDS: AHMC application standards including but not limited to the Evident Suite of applications and Microsoft Office Suite (Word, Excel, Access, Publisher, Outlook, and PowerPoint). All license documentation and original application media are documented and stored in the IS department. Installation of personally owned personal computer hardware or application is strictly prohibited. Any violations of software license agreement are reported to hospital administration.

HIPAA PRIVACY/SECURITY – INCIDENT REPORTING: All suspected violations of either the HIPAA Privacy Rule or HIPAA Security Rule must be reported immediately so that appropriate corrective action taken and reporting to the necessary agencies made. For suspected privacy violations (inappropriate handling or release of protected health information), please contact the Director of Health Information Management and provide them the details of the disclosure. For security violations (a password or other control has been compromised), please contact Information Services department representative. If urgency mandates an after hours notification, contact the hospital PBX operator who will have access to emergency contact information.

ISSUED PERSONAL COMPUTERS AND ELETRONIC STORAGE MEDIA: Storage of Electronic Protected Health Information data on unencrypted removable media, including but not limited to CD/DVD, USB removable flash drives or hard drives, floppy disks, etc. is prohibited unless authorized by the information Security Officer. If authorized, EPHI data may be stored on removable media provided either the device provides encryption capability via AES or other strong encryption algorithm, or the data is encrypted prior to storage using AES or other strong algorithm (e.g. using PGP or encryption software). Configuration of any hospital systems applications including but not limited to email, virtual network computing, remote desktop connection, etc. on any mobile device is prohibited unless authorized by the information Security Officer. Hospital employees using hospital-issued laptops must take reasonable precautions to protect the equipment from theft. Reasonable precautions include to not leaving the device unattended in a vehicle; installation of unapproved software on any Hospital system is prohibited. This includes, but is not limited to, game software, file sharing programs (e.g. LimeWire, Torrent), remote control software (e.g. PCAnywhere, GotoMyPC, LogMein), etc. Installation of unapproved software consume valuable system resources and create PC instabilities. If detected, Internet access will be disabled, the department manager will be notified and recurring issues will be brought to the attention of hospital administration. A listing of approved software products is maintained by the Information Systems Department. Inappropriate use of Internet access or the downloading of "shareware" programs is strictly prohibited and will result in disciplinary action, up to and including termination. If detected, Internet access will be disable, the department manager will be notified and recurring issues will be brought to the attention of hospital administration. Information Services assets are to be used to support AHMC business processes. To ensure this, detailed activity logging is maintained for each workstation that accesses the Internet.

ELECTRONIC MAIL ACCOUNT: Your AHMC email account should not be associated with personal use. Banking/credit account notices and the like should not be linked to the address. Personal photos, distribution of jokes, chain letters, video clips, "Flash" content and the like are not permitted. If detected, your Internet email access will be removed without notice. If you receive unsolicited messages with the above mentioned content, notify IS with the senders address and it will be blocked.

AHMC is the sole owner of all information stored on the transmitted using their electronic systems, including email. AHMC reserves all rights to monitor electronic communications by its employees on its privately owned systems.

AHMC Anaheim Regional
Medical Center

Systems Access Request Form

Last Name: _____ Job Title: _____

First Name: _____ ROLE: ☐ **INSTRUCTOR**

Middle Initial: _____ ☐ **STUDENT**

☐ **REGISTRY**

ROTATION END DATE: _____

Registry/School: _____ (If Student OR Long-term Contract Only)

System Access Request:

☒ OMNICELL

☒ EMR

I have read and understand the content of the above Security Statement and agree to accept and abide by the policies.

User Signature: _____ Date: _____

CNO/Designee Name: _____

CNO/Designee Signature: _____ Date: _____