

HUMAN RESOURCES

Title : _____ Badge # : _____

USER

Start Date of User _____ / _____ / _____ **These Are Required Fields**

First Name : _____ MI : _____ Last Name : _____

Department : _____ Room : _____ Last 4 Digits of SS# : _____

Phone / Extension / Pager : _____ ECMCC Payroll? Y N If No, Employer _____

PC # _____ LP # _____ Cost Code _____

REQUIRED APPLICATIONS (PLEASE COMPLETE ONLY APPLICATIONS NEEDED FOR THIS EMPLOYEE)

Meditech New Name Change Revision to existing account

Set account up like : _____ Profile : _____ Care Provider Type : _____

Graduation Date or Expiration Date from your current title : (For non-credentialed titles only) _____

Title : (Circle one) Credentialed Titles : Attending Nurse Practitioner Physician's Assistant
 Non-Credentialed Titles : Fellow Resident Medical Student
 Other : _____

Primary Service :

- | | | |
|---|---|--|
| <input type="checkbox"/> Anesthesiology | <input type="checkbox"/> Laboratory Medicine | <input type="checkbox"/> Psychiatry |
| <input type="checkbox"/> Cardiothoracic Surgery | <input type="checkbox"/> Pathology | <input type="checkbox"/> Chemical Dependency |
| <input type="checkbox"/> Dentistry | <input type="checkbox"/> Neurology | <input type="checkbox"/> Radiology |
| <input type="checkbox"/> Dermatology | <input type="checkbox"/> Neuro-Surgery | <input type="checkbox"/> Rehab Medicine |
| <input type="checkbox"/> Emergency Medicine | <input type="checkbox"/> Obstetrics and Gynecology | <input type="checkbox"/> Chiropractic |
| <input type="checkbox"/> Family Medicine | <input type="checkbox"/> Ophthalmology | <input type="checkbox"/> Surgery |
| <input type="checkbox"/> Internal Medicine | <input type="checkbox"/> Oral and Maxillo-Facial Surgery | <input type="checkbox"/> Urology |
| <input type="checkbox"/> Acute Geriatrics | <input type="checkbox"/> Orthopaedic | |
| <input type="checkbox"/> Cardiology | <input type="checkbox"/> Podiatry | |
| <input type="checkbox"/> Hospitalist | <input type="checkbox"/> Otolaryngology | <input type="checkbox"/> Skilled Nursing |
| <input type="checkbox"/> Renal | <input type="checkbox"/> Plastic and Reconstructive Surgery | <input type="checkbox"/> Other _____ |

ESign Y N (Access to Electronic Signature)

Attending with Electronic Signature :

List those Attendings who may sign for you in your absence (Alternatives) :

Quantros

User has signed Computer Access Policy on file Y N

Active Directory and Email Accounts

Set account like : _____
 (Please write name of person who does the same job)

Outlook Account Y N Webmail Account Y N

Affiliate Y N (Access from outside clients to Meditech) Single Sign-On Y N

Other Access: _____

Omnicell (Unit Based Drug Cabinet)

Professional Title : _____ Template : _____

Nursing Supervisor Signature _____ Pharmacy : _____

Healthenet (Western New York Healthenet / PCI)

Birthdate : _____ / _____ / _____ Choose only one of the listed access setups

Access Required : Eligibility Y N Claim Status Y N Referrals Y N

Valco

Do you require Scanning? Y N

Meditech account name : _____ Do you work in Pharmacy? Y N Pharmacy Scanning? Y N

PACS / Amicas

Justification for Access : _____

Form 359 (Check your Group)

- | | | | |
|--|---|---|--|
| <input type="checkbox"/> Administrator | <input type="checkbox"/> Eye | <input type="checkbox"/> PACU | <input type="checkbox"/> Spine Center |
| <input type="checkbox"/> Admissions | <input type="checkbox"/> Head & Neck / Plastic & Reconstructive Surgery | <input type="checkbox"/> Surgery | <input type="checkbox"/> VAC |
| <input type="checkbox"/> Cardiology | <input type="checkbox"/> Internal Medicine | <input type="checkbox"/> Psychiatry | <input type="checkbox"/> WNY BH |
| <input type="checkbox"/> Chemical Dependency | <input type="checkbox"/> Obstetrics & Gynecology | <input type="checkbox"/> Rehab Medicine | <input type="checkbox"/> Other : _____ |
| <input type="checkbox"/> Cystology | <input type="checkbox"/> Oral / Max | <input type="checkbox"/> Renal | |
| <input type="checkbox"/> Electroconvulsive | <input type="checkbox"/> Orthopedics | <input type="checkbox"/> Sinus | |

TeleTracking Department : Circle One ACC / ADMIN / ADMISSIONS / BHU / CASE MGR / CATH LAB
 DISCH PLANNER / ED / ENVSVCS / PACU / TRANSPORT / UNIT MGR / OTHER : _____

Location : _____ or Nursing Unit : _____

Title : _____ Set up like : _____ (user performing same duties)

Allscripts

- Attending PA NP Fellow Resident RN LPN MOA Clerical
 Clinic Supervisor Med Student Billing View Only Other _____

Email : _____

Location

Site / Clinic : _____

Other : _____

For Attending, PA, NP (HIS Use Only)

DEA # _____ Exp. Date : _____

License # _____ Exp. Date : _____

NPI # _____ Resource Code : _____

Provider Specialty : _____

Check off box for Account Creator (HIS Use Only)

- | | | | |
|---|---|-------------------------------------|--------------------|
| <input type="checkbox"/> Active Directory | <input type="checkbox"/> Other Access | <input type="checkbox"/> Valco | Created By : _____ |
| <input type="checkbox"/> User Account | <input type="checkbox"/> Meditech | <input type="checkbox"/> PACS | |
| <input type="checkbox"/> Mail | <input type="checkbox"/> Credentialing Software | <input type="checkbox"/> TeleTrack | Date : _____ |
| <input type="checkbox"/> Affiliate | <input type="checkbox"/> Provider Dictionary | <input type="checkbox"/> Form 359 | |
| <input type="checkbox"/> Esign | <input type="checkbox"/> Omnicell | <input type="checkbox"/> Quantros | |
| <input type="checkbox"/> SSO | <input type="checkbox"/> Healthenet | <input type="checkbox"/> Allscripts | |

Purpose

It is the policy and practice of the ECMCC Network to protect its computer hardware, data, software, and other information assets. To accomplish this, it is necessary to set restrictions and limitations on the disclosure of and access to these assets.

The purpose of this policy is to provide the framework for providing data on a need-to-know basis so information can be protected from unauthorized disclosure. This framework will minimize the potential loss of public confidence, disruption to internal operation, unnecessary expense, competitive disadvantage, and ensure compliance with regulatory requirements such as The Health Insurance Portability and Accountability Act (HIPAA). This policy is intended to provide guidance and all ECMCC Network workforce are expected to apply and extend these concepts in their day-to-day employment activities.

Application

The "ECMCC Network" is comprised of the Erie County Medical Center Corporation, Clinics, and the Erie County Home.

This policy applies to the workforce at the ECMCC Network and includes; employees, medical staff, contractors, students and volunteers.

Use for Business Purposes

The computers, network, Internet connections, software applications and e-mail systems (collectively referred to as "computer systems") available to the workforce are intended to support the business of ECMCC Network.

Computer systems are to be used for business purposes only.

Confidential Information

The ECMCC Network computer system includes confidential records of protected health information (PHI) as defined by the Department of Health and Human Services, Title II, Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The ECMCC Network has the legal and ethical obligation to safeguard this information. Workforce members are required to follow the ECMCC Network policies and procedures regarding the use and disclosure of PHI. This includes access to the minimum necessary data to accomplish day to day tasks such as treatment, payment, and operations. Access to records is restricted to the minimum necessary and is limited to that required to enable a user to perform his or her work for the ECMCC Network.

User ID and Password

System access is granted on a need-to-know basis. Workforce members will be issued a unique and confidential user ID and password. Access codes may not be shared, disclosed or used by any one other than the assigned individual.

Security

Any breach of security, including but not limited to, sharing access codes, passwords or wrongful access of any kind is a violation of ECMCC Network policy and may result in criminal prosecution under applicable computer crime laws. Workforce members who violate this policy will be subject to disciplinary action up to and including dismissal. The ECMCC Network will report violations of this policy to the appropriate law enforcement agency.

Use of ECMCC Personal Computers

ECMCC has purchased the right to use software on personal computers owned by the ECMCC Network. Software is subject to Federal Copyright protection and copying is strictly prohibited.

All printed information and data storage media including, but not limited to microfiche, optional and magnetic storage media, such as tape, diskette or fixed disk, is the property of the ECMCC Network and may not be shared, distributed, maintained or stored for use other than for ECMCC Network business.

Data created on ECMCC Network systems remains the property of the Network

Patient information in any format must remain on the property of the ECMCC Network unless appropriate authorization has been obtained.

Prohibited Activities :

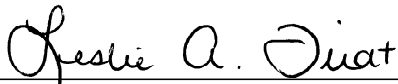
This list is intended to provide examples of computer access activities that are prohibited at the ECMCC Network. It is not intended to be an exhaustive list.

- ❖ Providing information about employees or patients to outside organizations without prior written approval
- ❖ Unauthorized use of computer hardware or software that is protected by copyright, trade secret or patent
- ❖ Unauthorized copying or distribution of copyright material, including digitalization and distribution of magazines, books, photographs, music or other material
- ❖ Export of software, technical information, encryption software, technical information or technology
- ❖ Introduction of malicious programs into the network, desktop or server such as a computer virus
- ❖ Use of your user ID and password by others
- ❖ Use of ECMCC Network assets to transmit or engage in violent, sexual or hostile activities
- ❖ Transmission of fraudulent offers or claims
- ❖ Any form of network monitoring that could intercept data

I further agree to the following :

- ❖ My User ID and password are equivalent to my legal signature and I will not disclose this information to anyone or allow anyone to access the system using my sign-on information.
- ❖ I am responsible and accountable for all entries and all retrievals accessed under my User ID and password. Any data available to me will be treated as confidential information.
- ❖ I will only use my User ID and password.
- ❖ I will access only the minimum necessary data I have responsibilities for.
- ❖ I will keep my User ID and password confidential. If either is compromised, I will immediately change my password and notify the helpdesk.
- ❖ I will not disclose any confidential information unless required to do so in the official capacity of my employment. I also understand that I have no rights or ownership interest in any confidential information.
- ❖ I will not leave a secured computer application unattended. I understand that my use of systems will be periodically monitored to ensure compliance
- ❖ I agree not to use the information in any way detrimental to the organization and will keep information confidential.
- ❖ I agree that disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship unless specifically waived in writing by an authorized party.
- ❖ I agree to return or destroy any data, software or other ECMCC Network property upon termination of my employment.

Questions about this Computer access policy should be directed to :
CIO, ECMCC Healthcare Information Systems at (716) 898-5584



Leslie Feidt, Chief Information Officer, Erie County Medical Center



Jody Lomeo, Chief Executive Officer, Erie County Medical Center

Purpose

The purpose of this policy is to establish principles to guide the Erie County Medical Center Corporation (ECMCC) in its endeavor to promote and enforce appropriate use of the Internet.

This policy is in accordance of the Technical Safeguard 164.312 (e) (i), Transmission Security and the General Security Rules 164.306 of the Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rule

AUTHORIZATION PROCESS

The following accounts may be established for Internet access.

ECMCC - Individual User Account. An individual user account is established when an ECMCC employee requires access to the Internet to perform his job responsibilities.

Non-ECMCC Employee Request. A non-ECMCC Affiliate may request Internet access through the ECMCC Network. ECMCC will not be liable for activities and or transmission of data that occurs from this account. Costs associated with this service will be billed on a yearly basis to the non-ECMCC Affiliate. ECMCC is not responsible to monitor appropriate use or assist with desktop configuration.

For all account types, a Computer Access Application must be completed with signature from the senior or executive management. This form will be submitted to the IT department for processing.

Additional hardware and software may be required for an Internet request. If so, additional authorization will be required by the Senior Manager. The IT department will install, test and maintain Internet access on ECMCC standard computers. Internet access can be made available through any standard workstation on the ECMCC network. Based on security risk, Internet access through modem dial up is prohibited.

ACCEPTABLE USE

Connection to the Internet is an ECMCC network service provided by the Information Technology Department (IT) that enables authorized personnel to access Internet resources for business users only. This includes the World Wide Web. Inappropriate use of the Internet, as defined below, is not permitted. Those users accessing the Internet for inappropriate purposes during their work hours will be subject to ECMCC's progressive discipline policy and access privileges may be terminated.

The following activities are considered unacceptable and inappropriate use of the Internet.

- The creation, download, storage, copying, or transmission of sexually explicit materials, materials or remarks that ridicule others on the basis of race, creed, religion, color, sex, handicap, national original or sexual orientation, materials related to gambling, illegal weapons, terrorist activities, etc., chain letters, broadcast transmissions, or other mass mailings.
- Use for commercial purposes or in support of "for profit" activities (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services)
- Use of the Internet in a way that results in unauthorized charges or expenses to ECMCC.
- Any attempt or action aimed at damaging, disabling or interfering with the normal operation of ECMCC Internet access or the ECMCC home page, including the hardware and software serving or connected to same.
- Use of personal web-based e-mail products such as hotmail.com or yahoo.com
- Violating copyright laws.
- Use of the Internet that violates state for federal law or regulation, including copyright laws.
- Internet usage that causes disruption of service to ECMCC Network due to utilization of high bandwidth. This includes large files (sound and streaming video), push technologies and other continuous data streams.

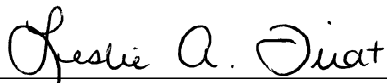
Downloading of data from the Internet (WWW, FTP, Gopher, etc) or from bulletin boards and Usenet sites for ECMCC business purposes only is permitted. The downloading of software applications requires prior approval and licensing of the IT Department. The IT Department will not support non-authorized applications. To request the installation of a software program downloaded from the Internet you must complete a Request for Service form as outlined in the Request for IT Service Policy.

All data downloaded form the Internet must be immediately scanned for virus following the ECMCC Antivirus Policy. Critical data should be stored on the ECMCC Network for backup purposes.

Transmission of unsecured corporate sensitive or Protected Healthcare Information (PHI) through the Internet is prohibited. Upon request, the IT Department will provide a secured method of transfer for all corporate sensitive data or PHI.

Monitoring

The IT department will monitor Internet access and usage for the same reasons and purposes as it monitors and ECMCC computer device or electronic information. ECMCC reserves the right to discontinue services, as it deems appropriate.



Leslie Feidt, Chief Information Officer, Erie County Medical Center



Jody Lomeo, Chief Executive Officer, Erie County Medical Center

REMOTE ACCESS POLICY



ACCEPTED USAGE :

Remote access is provided to users for use from home for business purposes only. Use of remote access is governed by current ECMCC Confidentiality and Security Policies. Resources used are the property of Erie County Medical Center Corporation and considered confidential. As such, this information shall not be shared, distributed, maintained, or stored in a careless manner.

ECMCC has purchased the right to use software on personal computers, both on and off the ECMCC local area network. This software is protected by federal copyright laws. At the time of employment termination or when remote access is no longer deemed necessary to your specific job function, the remote access software must be installed from your computer. Removal of this software is your responsibility.

DISCLAIMER :

ECMCC is not responsible for damage to systems on which the client is installed. The distribution media has been verified to be virus free and the installation process tested. ECMCC is not responsible for technical support outside of the realm of connection or applications issues.

By signing below I have read and agree to abide by the following ECMCC policies :

- **Computer Access Policy**
- **Internet - Authorization and Acceptable use Policy**
- **Remote Access Policy**

Print Name : _____

Signature : _____

Date : _____

Clinical Director / Senior Manager

Print Name : _____

Signature : _____

Date : _____