Community HOSPITAL

COMPUTER INFORMATION SECURITY ACCESS USER REQUEST/CHANGE FORM

The Information Security Access form is necessary to grant access for employees or external persons to Community Hospital's medical information system(s). Please fill out each pertinent section of the form **entirely**. Each supervisor will need to **mark** the necessary access, **sign** the security form, and **return** it to Community Hospital's I.T. Department.
Employees of Community Hospital will sign their form and receive their account information in orientation.
All external users will be notified via email, phone, or courier to the contact information provided on the form.
Access **will not** be given to a hospital system without the completion of this form.
*****Once completed, please fax the Information Security Access form with the appropriate signatures to 970-644-3519. If you have any questions, contact us at 970-644-3500.***

Date:

*First Name: * MI: *Last Name:

Applicant is:
□ **Employee** □ **Contractor**
□ **Volunteer** □ **Physician Office Staff**
□ **Student** □ **Intern**

EMPLOYEE/VOLUNTEER INFORMATION – To be filled out by Community Hospital Only

Current User: □ **Yes** □ **No**

□ New Employee □ Rehire
□ Dual Status □ Change

Start Date:

Employee Status:
□ **Full Time**
□ **Part Time**
□ **Pool/PRN**

Job Position:

Department:

Employee Number:

Department/Position or Name Change:
From: ________________________ to ________________________

EXTERNAL USERS INFORMATION ONLY – Outside offices/Contractors please complete all info

Company/Practice Name: Supervisor:

Address:

Phone Number:

Email Address:

Date of Birth:

Title:

STUDENT NURSE

Name of School: Program: Site:

Dates of Rotation:

**PROGRAM ACCESS REQUESTED – Check all boxes necessary for job duties and write in user to mimic

□ **Meditech**
□ **Email**
□ **Windows**
□ **Allscripts**

□ **QuickChart**
□ **Medex**
□ **QuickScan**
□ **Philips iSite (PACS)**

□ **Greenway**
□ **TOC**
□ **Remote Access**
□ **SIS (see SIS form)**

□ **Other Request**
____
____

**** Mimic access profile of this user: ________________________________**

INFORMATION TECHNOLOGY/HR ONLY:

Actions Taken	**Date**	**By**
Organization/Vendor Checked Against Exclusions List		
Applicant Checked Against Exclusions List		

I, ____, have read and agree to abide by the attached guidelines.
Please print

Applicant Signature: ____ Date: ____________________________

Supervisor Signature: ____ Date: ____________________________

Community Hospital has the right to restrict or terminate Internet access at any time for any reason. Community Hospital further has the right to monitor Internet activity (including Internet E-mail) to maintain the integrity of the system. Rev. 1/2016

Community HOSPITAL

INFORMATION SECURITY ACCESS REQUEST GUIDELINES

Security

Access is provided to Community Hospital's computer network and medical information systems for all physicians and employees who need access in order to perform their job duties. Please read and agree to the following important stipulations regarding access to patient information and computer systems belonging to Community Hospital.

1. Network login passwords, Meditech passwords, and any other system passwords are not to be shared with any other person, staff or otherwise. It is prohibited for you to access any computer system utilizing the login of another user. You have security permissions based on who you are and the information you need to access. You cannot log on to the system and then allow someone else to use your login.
   I agree to maintain the security of my login information.

2. Passwords will expire on a regular basis, usually every 90 days. This allows us to maintain a level of security in keeping with internal requirements and expectations. I agree to change my password sooner should I have reason to believe my password has been compromised and notify the Information Technology of same.

3. When you have completed your work on the system, it is necessary to log off your PC or terminal. Since the Meditech system records activity based on user login, this will avoid the possibility of other people having access to the system and recording information using your login.
   I agree to log off any time I leave the area and/or lock my pc.

4. An employee involved in dictation and on-line review of patient notes is given an electronic signature to affix to these notes in the computer. When you affix your electronic signature, you are agreeing that you have reviewed the dictated information and agree to its accuracy and integrity.

5. All patient information is confidential. Any use of computerized patient information, for other than patient treatment, payment or operation purposes is prohibited. The Office of Civil Rights may impose substantial penalties or imprisonment for HIPAA related violations. Inappropriate access may result in disciplinary action up to, and including, separation from employment.

6. Installation or removal of any software or hardware is only to be performed with express permission from IT.

7. **To access your own medical records, you must request them via Health Records Information Services (HRIS). Accessing your own records, or those of another person for reasons other than performance of job duties, is not permitted and may result in disciplinary action and/or separation of employment.**

Internet

8. Usage of the Community Hospital Internet system at work must be for work-related communication, research and education.

9. The Internet is a global network and therefore it is impractical to control the content available to any one user. I.T. promotes the responsible use of the information that exists on the Internet. We acknowledge that inappropriate information and web sites exist and we require that our users avoid these sites (such as sexually explicit web sites, etc.).

10. I.T. reserves the right to audit any activity of any user at any time. Internet email is the property of Community Hospital, not the user. Community Hospital reserves the right to read any email for any user as necessary. There is no reasonable expectation of privacy for Employees when using Internet email.

Community Hospital has the right to restrict or terminate Internet access at any time for any reason. Community Hospital further has the right to monitor Internet activity (including Internet E-mail) to maintain the integrity of the system. Rev. 1/2016

INFORMATION SECURITY ACCESS REQUEST GUIDELINES

11. Internet email accounts will be monitored for inactivity and storage limits. Email accounts that have been inactive for 180 days may be deleted due to lack of use. Any user whose mailbox size is greater than 1GB may be asked to archive or delete items in their mailbox.

12. Access to all Community Hospital systems will be terminated when an individual ceases to be an Employee Partner of Community Hospital or its subsidiaries.

13. Please use discretion/caution in providing any personal information via the Internet. You cannot be guaranteed privacy when using the Internet. The transmission of any patient related information is strictly prohibited unless specifically authorized by the Information Technology department, and that information is encrypted.

14. The transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for product advertisement or political lobbying is not consistent with the purposes of Community Hospital Internet access. Illegal activities are strictly prohibited. Conducting any type of personal business enterprise whether for profit or non-profit is prohibited.

15. Community Hospital declares that unethical/unacceptable behavior or usage of the Internet System is just cause for taking disciplinary action. Inappropriate activities may include, but are not limited to the following:

    - Uses the network for any illegal activity, including violation of copyrights or other contracts violating such matters as institutional or third party copyright, license agreements and other contracts;
    - Intentionally disrupts network traffic or crashes the network and connected systems;
    - Degrades or disrupts equipment or system performance;
    - Uses the Community Hospital computing resources for commercial or financial gain or fraud;
    - Steals data, equipment, or intellectual property or seeks to gain unauthorized access to resources or data;
    - Forges electronic mail messages, or uses an account owned by another user or invades the privacy of individuals;
    - Posts anonymous messages;
    - Downloads, installs, or executes security vulnerability programs or utilities which are designed to reveal weaknesses in the security of the Community Hospital system, or any other system.

Remote Access

16. Community Hospital has enforced a 30 minute idle timeout that terminates a connection due to inactivity. Please terminate Remote Access connection when work is completed.

17. Users of Remote Access must provide their own internet connectivity. Connection speeds will vary based on limitations of their internet service provider.

18. **At no point, should the user's equipment (i.e. laptop, cell phones, personal computers, etc.) contain any electronic protected health information (ePHI).**

19. When connected via Remote Access, internet browsing is not available.

If any of the above guidelines are not followed, your computer access may be suspended and/or you may be subject to disciplinary action up to and including separation of employment.

Community Hospital has the right to restrict or terminate Internet access at any time for any reason. Community Hospital further has the right to monitor Internet activity (including Internet E-mail) to maintain the integrity of the system. Rev. 1/2016