

MEDICAL CENTER HOSPITAL SECURE LINK REMOTE ACCESS

First three pages are for Vendor records; please do not return with application.

**** Please email the completed form to 1385@echd.org ****

In order to comply with Medical Center Hospital policy 1044 regarding remote access to the hospital computer systems, please fill out, print and sign the form below. Policy 1044 requires all users to submit access requests in writing to the Information Technology Steering Committee. Medical Center Hospital reserves the right to do random reviews and spot checks to ensure compliance with this policy and proper patient confidentiality is being maintained. Medical Center Hospital is not responsible for maintenance of any hardware or software. A computer security agreement must be signed before access can be obtained.

Minimum requirements for a Secure Link virtual support network (VSN) connection:

It is your responsibility to have anti-virus software installed and to keep it updated.

1. A company email address. ISPs like Yahoo, gmail, hotmail etc., are not allowed.
2. Microsoft Internet Explorer
3. Windows XP or better
4. Broadband internet connection

STRONG PASSWORD RULES

MCH is serious about protecting patient privacy. Passwords are the entry point to our network, so they must be strong. A weak, stolen, or misused password can give intruders or unauthorized people access to information they have no right to know.

Strong password Do's and Dont's:

- Do make your password 7 or more characters long
- Don't have a password that contains any part of your name
- Don't use terms that anyone familiar with you could guess
- Don't include personal information, names, addresses or phone numbers.
- Avoid words that are in the dictionary as these create weaker passwords.
- Include mixed case, numbers, and punctuation in the password. These increase the password's strength.
- You can make a password stronger without making it longer by breaking up alphabetic characters with numbers and punctuation. Using mixed case within strings of alphabetic characters is also helpful.
- Use a passphrase rather than a password. A passphrase is difficult for an attacker to guess. Including misspelled words in the phrase makes it an even stronger password. (i.e. Igo2colege; Iwerk4MCH.)

To create a strong password, use 3 of the 4 character classes listed below:

- Upper Case
- Lower Case
- Numbers
- Special Characters

Examples of strong passwords:

<u>Original Password</u>	<u>Strong Password</u>
CocoBeach	CoCo_Beach
UpdateRecords	Upd8Rec\$
I work for MCH	Iwerk4MCH

Ideas for passwords might come from a phrase such as “A good password is hard to figure out.” This could be translated into a strong password such as “Agpih2f0”

Letters can also be substituted for numbers (and vice versa) by other sets of simple rules. For instance: 1 looks like a lowercase letter L; 2 looks like a Z; 3 looks like a backward E; 4 looks like an A; 5 looks like an S; 6 looks like a G; 7 looks like a T; 8 looks like an R; 9 looks like a backward P; and zero looks like an O.

To make all of your passwords at MCH compatible, start your password with a letter.

POLICY MEMORANDUM

POLICY SUBJECT:	Remote Access of Hospital Computer Systems
POLICY NUMBER:	MCH-1044
JCAHO FUNCTION AREA:	Leadership
POLICY APPLICABLE TO:	All Users of MCH Computer Systems
POLICY EFFECTIVE DATE:	January 24, 1995
POLICY REVIEWED:	12/1/97; 11/20/00; 3/4/02; 1/29/07
POLICY REVISED:	12/1/97; 3/23/01; 1/20/05; 4/26/07
POLICY STATEMENT:	
<ol style="list-style-type: none">1. All computer users who need remote access to any Medical Center Hospital (MCH) computer system must submit a Secure Link Access Request Form. This form must be submitted to the Chief Information Officer for approval. Once approval is given, instructions for setting up the Secure Link account will be provided to the user. The necessary forms can be obtained from the I.T. Department or from the MCH Intranet.2. MCH reserves the right to do random reviews and spot checks to ensure compliance with policies and procedures and to ensure proper patient confidentiality is being maintained.3. Anyone requesting remote access must supply their own computer equipment.4. MCH will provide instructions for configuring the Secure Link account.5. Safety and security of the computer and information accessed is solely the responsibility of the user.6. MCH employees using computer equipment remotely must have completed PC Orientation and training on the applications they will be using.7. Remote users are bound by the same rules that apply to personal computers used at MCH.8. Remote users will be required to change their passwords according to the rules governing the application(s) being used.9. MCH does not condone, allow or accept responsibility for unauthorized, unlicensed or pirated software.10. MCH is not responsible for maintenance of any hardware or software used in conjunction with Secure Link.11. The use of regularly updated anti-virus protection is required12. The Secure Link Access Request Form must be signed before access can be obtained.	

AUTHORIZING SIGNATURE(S)	
	William W. Webster Chief Executive Officer
END OF POLICY	

TO:

FROM: Gary Barnes, Chief Information Officer

As a vendor under contract at Medical Center Hospital, it is reasonable to believe that you might come in contact with or view patient information. Information from any source and in any form, including paper records, oral communications, audio or electronic recordings is strictly confidential.

Vendors will not intentionally attempt to gain access to information that is not needed for the scope of their project.

Vendors will not attempt to access or connect to systems that are outside the scope of their project.

Vendors will not access any MCH system, nor make changes to any MCH system, without prior approval from the appropriate MCH application analyst.

Connection to the MCH system will not extend beyond the length of time it takes to complete the pre-approved work.

All materials provided to the vendor by MCH or gathered by the vendor during their work project are to be used strictly for the uses spelled out in the project and are to be returned at the end of the project. No copies may be made outside of the scope of the job by you, your employees, your partners, your business associates, your friends, families, acquaintances or any other person.

MCH reserves the right to monitor and monitoring does occur. MCH may, review, audit, intercept, access and disclose all matters on MCH computers at any time, with or without prior notice and that such access may occur during or after working hours. The use of a password or security code on a computer system does not restrict the right of MCH to access electronic communications.

Violations of this policy may constitute grounds for termination of your contractual relationship or other terms of affiliation with Medical Center Hospital. Unauthorized release of confidential information may also have personal, civil and/or criminal liabilities and legal penalties.

I have read and agree to comply with the terms of the above statement and MCH Policy 1044 (Remote Access of Hospital Computer Systems.)

Printed Name

Signature

Title or Company

Date

Purpose for Access

Sponsoring Department within MCH

SECURE LINK ACCESS REQUEST FORM

Your Organization/Company Name _____

Your MCH I.T. Contact Name _____

Name _____ Business Phone _____

Business Address _____

City _____ State _____ Zip _____

Email Address _____

Personal I.D. **Generally the requesters drivers license number or any other number that we can use to verify the persons identity _____

Reason Access is needed: _____

_____/_____
Signature of Vendor Representative Date

_____/_____
Signature of MCH I.T. Contact Date

Mail to: Chief Information Officer
Medical Center Hospital
P.O. Drawer 7239
Odessa TX 79760

OR Fax to: 432-640-1378

Please print and return this completed, signed form to:

CONFIDENTIALITY AGREEMENT AGENCY PERSONNEL

This Confidentiality Agreement (hereinafter referred to as “Agreement”) is entered into by and between _____ (Name of Contractor, hereinafter referred to as “Contractor”), and Medical Center Hospital (hereinafter referred to as “MCH”), collectively referred to as “the Parties.”

Contractor, an employee of _____ (Name of Agency), providing patient care at MCH will have access to and review confidential patient information maintained in electronic and/or paper form by MCH.

Contractor acknowledges that Contractor has reviewed the MCH Data Policy and agrees to abide by MCH's Data Policy as adopted and amended from time to time.

Contractor acknowledges and understands that unauthorized access, use, disclosure or reproduction of any patient information in violation of MCH's Data Policy or in violation of this Agreement will authorize MCH to prohibit them from providing any patient care on MCH's premises. Contractor further understands that certain unauthorized disclosure of patient information is punishable by fines and penalties imposed by Federal and State law(s).

Contractor further understands and agrees not to access, disclose or reproduce any confidential patient information other than as necessary to fulfill Contractor's obligation to provide patient care.

Contractor further agrees to notify MCH of any violations of any use of or disclosure of confidential patient information not provided for by this Agreement.

Contractor acknowledges and understands that if Contractor is granted specific computer system(s) access based on the nature and scope of Contractor's assignment, Contractor is prohibited from accessing or attempting to access any computer system(s) in a manner that violates MCH's Data Policy or is not consistent with my specifically assigned user rights.

Contractor agrees to use appropriate safeguards to prevent use or disclosure of confidential patient information other than as provided herein. Nothing herein shall preclude Contractor from making available to a patient his or her confidential patient information when appropriate for continued patient care.

Upon completion of my assignment with MCH, Contractor agrees to return any confidential patient information in Contractor's possession.

Contractor agrees that in the event any amendments or corrections are made to the patient's protected health information such amendments or corrections will be incorporated into such records in Contractor's possession.

Upon request, Contractor agrees to make available Contractor's internal practices, books, and records relating to use and disclosure of protected health information to the Secretary or an employee of the Department of Health and Human Services.

I HAVE READ AND FULLY UNDERSTAND THIS AGREEMENT.

Representative of Medical Center Hospital

Contractor's Signature

Date

Date