



ICC Policy Regarding User Access to and Usage of the I-Care System
Final Version 5/05/03

The I-Care System is a web based MPI/CDR containing sensitive Protected Health Information (PHI) to be shared between the ICC members (both physician and non-physician personnel). I-Care users will abide by the following guidelines as conditions to gaining access to the secure system.

Purpose

- To establish an overall security policy to protect electronic information assets.
- Assign user accountability and responsibility for the protection of electronic information assets.
- Demonstrate the ICC's accountability and responsibility for the establishment and enforcement of appropriate security measures to protect electronic information assets.

General

- The I-Care system will only be accessible by ICC staff, ICC members' clinical staff and Travis County Medical Society's Project Access Doctors.
- The ICC member will identify I-Care users at each location.
- The ICC member will identify I-Care users' security levels.
- All users of the I-Care system must be thoroughly trained on ICC Privacy and Security Policies.
- Access to the I-Care system is via the Internet. The ICC Security Officer will assign a user login and password to the user in order to gain access to the I-Care system.
- Users are only permitted to use and share visual and/or printed patient information to perform their job duties.
- Users will be required to abide to the I-Care policies and procedures to protect the confidentiality and security of PHI. If a member's policy is stricter than the ICC's with respect to access at a particular location, users at that site must follow the member's policy as well.

User Logins and Passwords

- User logins and passwords will be exclusive to each individual user.
- User logins and passwords must be kept private and cannot be shared between users.
- User passwords will have a length of at least **8** characters.
- User passwords will expire after a **90** day period.
- User lockout occurs after **3** unsuccessful login attempts.
- I-Care Helpdesk personnel will not reissue passwords or unlock accounts without verifiable identification from the user. (Last four digits of user's social security #).
- All passwords should be changed if stolen or believed to have been compromised.
- Upon password expiration, the system will not allow a user to re-use previously used passwords.
- Users should not use their username or any other personal identifier as their password to gain access to the I-Care system.
- Users should logout of or lock the I-Care system when not in use and/or away from their desks.
- User login & password will be inactivated when a user terminates their position.
- Users needing assistance with system login/password should direct their issues to the I-Care Help Desk or the I-Care support email address.
- The I-Care Security Officer will keep a master log of all I-Care user ids and their corresponding user identifiers.

Privacy and Security

- Each user is responsible for ALL activity performed with their assigned user ID and password.
- A user's ability to view different levels of information within the I-Care system, from patient demographics to patient encounter information, will be established on a "need to know" or role supported basis.
- Computers and printed PHI materials should be kept in restricted areas that are not accessible to the public.
- Computer screens with client information should not be easily visible by people who are not authorized to see the information. The ICC may request that a member change the location of a computer if the opportunity for unauthorized access or observation exists.
- After **10** minutes of inactivity on the I-Care system, the user will automatically be logged off and must log back into the system to regain access.
- The I-Care system is accessed via the Internet; thus it can be opened from any computer with web access. Users should only access the I-Care system for work related activities established on a "need to know" basis.

Security Breaches

- The ICC Security Officer will generate I-Care audit reports on a monthly basis for review with the member regarding user accessibility and usage.
- Members and/or users must promptly report security incidents, but no later than 24 hours after the discovery, to the ICC Security Officer.
- Incident response procedures may result in interruption of I-Care web services if deemed necessary.
- User access privileges may be suspended if deemed necessary to maintain the integrity of the I-Care system.
- Once a user violation has been identified, the following steps will be immediately taken:
 - The ICC member who employs this user will be notified in writing by the ICC Security Officer within 5 days. The ICC member will determine disciplinary action (if any) for the violator and report back to the ICC Security Officer what actions have been taken, and what further actions may be necessary for either party to take to assure that no further violations occur.
 - The I-Care Security Officer will terminate the user's login and password (access to the system).
 - The I-Care Security Officer will perform an audit of the user's past system activity to conclude if prior infractions occurred.

Audit

The ICC will perform two types of audits on an agreed-upon schedule with each participating ICC member. One type of audit to be conducted is to assure that I-Care users are accessing data that they are only authorized to view. The second type of audit would be to verify authorization flags/revocation flags match up with the signed forms on file. The ICC will provide written reports of audit results to members, with recommendations for any improvements or follow-up needed.



ICC Procedures for Implementing User Access to and Usage of the I-Care System **Final Version 5/05/03**

The process the ICC will use to allow users access to the I-Care System is as follows:

I-Care System Usage and User Security Levels

- ICC Members (who have the authority) will provide a role based list of proposed user names as well as their security level to the ICC Security Officer. This information can be communicated via email or fax.
- The ICC Security Officer, for security level accuracy, will review and approve all I-Care user access request lists. The ICC Security Officer maintains the right to question requested user access security levels and to limit and/or deny access if deemed necessary.
- Users cannot be set up for access if the ICC Security Officer does not have:
 - An (copy or original) ICC User Access Policy and Procedure Document, with both user and supervisory signatures.
 - An identified security level for the user.
- If more than one ICC member requests access for the same user, the ICC Security Officer will contact all members proposing access to inform them of this. If the members do not propose the same level of access, the ICC will work with members to resolve the difference, and will only grant the lowest level of access until a resolution is achieved.
- Once user access is approved, the ICC Security Officer will set up the user's security level accordingly within the I-Care system "prior to their access".
- The ICC Security Officer will notify users of their assigned I-Care user id/password via telephone within 3 business days of receipt of request. Direct contact must be made between the ICC Security Officer and the user and they must verify their identity (last 4 digits of SS#) before login information is given out. If the user is unavailable when the ICC Security Officer calls, no messages will be left other than to notify the user to call the ICC Security Officer for this information.
- Users will gain access to the I-Care System via the following email address:
https://epicweb.ascensionhealth.org/ewiccprd/common/epic_login.asp
- Once the user initially logs into the I-Care system via their assigned user id/ password, they will be required to establish their own, unique user password to gain future access.
- The user will be trained on:
 - ICC Privacy and Security Policies
 - Gaining access to the I-Care system
 - Usage of the I-Care System
 - Their security level and access
- Users' should only view and use patient information as needed, with the intent of providing care to the patient and/or to perform their specific job duties.

Password Procedures

Users must take care in keeping their login and password private and secure. To ensure these measures:

- User passwords are to consist of at least **8** characters.
- Users should select a password that is hard to guess. Do not use a word that would appear in a dictionary. User selected passwords must be difficult to guess. Words in a dictionary, a derivative of the User ID and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouses' name, children's names, pet's names, license plate, SSN and birthday must not be used.
- Passwords should use a combination of alpha (not case sensitive), numeric, and punctuation characters.
- Whenever an authorized user has a reason to believe his/her password has been compromised, they should change their password. They should also do so whenever he/she is asked to do so by either a supervisor or the ICC Security Officer, whether or not a reason is given.

Users should not:

- Change their password while someone is looking over their shoulder.
- Leave their password in a place where they can be seen by anyone, such as labeled to your computer.
- Write their password on a piece of paper marked password.
- Use the same password for all applications they use. If someone finds or "cracks" the user's password, ALL of their access could be compromised.
- Use an obvious password, such as their name, their username, a blank password, the word "password" or any word that could be found in a dictionary.
- Give his or her password to someone else.
- Use someone else's login and password to gain access to the system.

Password Expiration

- User passwords will automatically expire after **90** days.
- Upon expiration, users will be prompted to change their password to gain I-Care access.
- Users should not input previously used passwords when prompted to change, they should be unique and follow the procedures listed under: Password Procedures.

Terminating User Access

When an active user of the I-Care system no longer needs access because they have changed positions, left their position or been terminated from their position:

- The ICC Member (or employee Supervisor) must notify the ICC Security Officer via phone/email/fax with the name of the user and the termination date.
- The ICC Member must notify the ICC Security Officer of user termination within a 24-hour period.
- The ICC Security Officer will terminate the user logon and password within 24-hours of notification.

Troubleshooting Policies

If the user is active, using the correct login and password to gain access to the I-Care system and the website is functioning, but they cannot gain access to the system

OR

If the user gets locked out of the system after **3** attempts of logging in, then the following response guidelines will be followed:

- If the user needs immediate response, they should call the I-Care Help Desk during regular ICC business hours at 927-6277, ext. 247. If a message must be left, users will get a response within a **3** hour period that same business day. Messages left after hours will be responded to on the next business day.
- A next business day (24 hour) response will be given if the user communicates their issue via the I-Care Help Desk email: support@icc-centex.org
- Users must identify themselves via an established user identifier (last 4 digits of user's social security #) when requesting help with user lock out or password re-issue. For security purposes, support will not be given without this information.

All other training issues, questions and concerns regarding the I-Care System can also be directed to the above phone number (for emergencies and immediate response) or the I-Care Help Desk email address.

Security Issues

Members and users must take extreme caution in keeping their access to the I-Care system secure. They must take the necessary measures to protect the patient information they have admittance to. If security is breached, the incident must be reported to the ICC Security Office as soon as possible (within a 24 hour period), either via telephone at 927-2677, ext. 247 or email at support@icc-centex.org.

The ICC Security Officer along with the Director of Technology will review the security breach incident to determine what plan of action is necessary to ensure system protection. The ICC will inform the member in writing of its concerns within 5 days and immediately take any steps it deems necessary, up to and including denying access to the I-Care system data to that member and its staff, until such time as its concerns have been addressed satisfactorily.

Security Issues, Cont.

The following list includes, but is not limited to, areas that constitute a breach of I-Care Security:

- Giving someone else your I-Care user id and login, regardless of whether this person already has access to the system or not.
- Using someone else's I-Care user id and login to gain access to the system.
- Loss of documented I-Care user id and password.
- Use of visual and/or printed patient PHI for purposes other than providing care for that individual and/or to perform job duties.
- Sharing the I-Care web address with non-users.
- Locating computers/computer screens with I-Care access in an area viewable by the public.
- User incorrectly identifies himself when calling The I-Care Help Desk for assistance with system access.
- User remains logged into the I-Care system when away from their computer, thus leaving the system vulnerable to access by unauthorized users.
- Not reporting the departing of a user with access, so their log-on can be deactivated.
- Flagging a patient record as "authorized" or "revoked" without having the required needed signed forms by the patient in place.

Audits

- User security levels limit the type of data viewed and have been designed to match typical roles. Prior to users gaining access to the I-Care system, the ICC Security Officer will verify they only have access to the screens allowed them as determined by their assigned security level.
- The ICC Security Officer will conduct a quarterly audit that matches up logged user access to the I-Care system with user work schedules. This will determine users are gaining access to the system during their working hours.

I-Care System Confidentiality Agreement

I have read and understand the above Policies and Procedures regarding access to and the usage of the I-Care System. I realize my user responsibilities of:

- Keeping the access I have to the I-Care system secure.
- Securing the PHI (Protected Health Information) I will be viewing and using for my specific role.
- The accountability I have in reporting I-Care security breaches to the ICC Security Officer
- Following the Patient Access Policies and Procedures as described in the Document.

By signing below, I agree to these terms:

Name of User	Signature of User	Date
--------------	-------------------	------

User's Title/Position	Assigned Security Level
-----------------------	-------------------------

Location	E-Mail Address
----------	----------------

Business Telephone Contact Number

User Identifier (Last 4 digits of Social Security #)

Name of Supervisor	Signature of Supervisor	Date
--------------------	-------------------------	------