



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>Information Systems</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>User ID's and Passwords</b>	<b>Revision Date:</b>	<b>4/20/05</b>
<b>Policy #:</b>	<b>ISP-002</b>	<b>Review Date:</b>	<b>6/26/08</b>
<b>Responsible Party:</b>	<b>Chief Information Officer</b>	<b>Revision #:</b>	<b>2</b>

---

**Scope:**

This policy is applicable to all users of any information system or application of Essent Healthcare, Inc. ("Essent").

**Purpose:**

The purpose of this policy is to set forth guidelines for assigning a unique user ID and password to each authorized user of the information systems of Essent.

**Policy:**

It is the policy of Essent that user names and passwords are unique to each user, must remain confidential, and must never be shared with any other individual. All system users are responsible for information accessed by their account. Any miss-use of information and/or breach of confidentiality is grounds for disciplinary action, up to and including termination of employment and/or civil or criminal prosecution.

Passwords will expire every 90 days (subject to system limitations) at which time the user will be prompted to change their password. Any user accounts with no activity for 120 consecutive days will be inactivated. Reactivation will occur only upon completion of Form ISF-001 "*Information System Access Request Form*".

All workforce members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines at all times:

1. Passwords are only to be used for legitimate access to networks, systems, or applications
2. Passwords must not be disclosed to other workforce members or individuals;
3. Workforce members must not allow other workforce members or individuals to use their password
4. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

All system users are responsible for reporting any incident of unauthorized access to their Facility Security Officer immediately.



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>Information Systems</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>User ID's and Passwords</b>	<b>Revision Date:</b>	<b>4/20/05</b>
<b>Policy #:</b>	<b>ISP-002</b>	<b>Review Date:</b>	<b>6/26/08</b>
<b>Responsible Party:</b>	<b>Chief Information Officer</b>	<b>Revision #:</b>	<b>2</b>

---

### PROCEDURE FOR MEDITECH (MAGIC sites)

Essent has standardized on MEDITECH (MAGIC) as the Healthcare Information Systems solution. All users are identified and authenticated via Login ID and Password in the MEDITECH system. Below is the format in which users are defined:

#### Login ID

Within the MEDITECH system, each user ID must be in alpha numeric and in the format of AAANNNN, where the three alpha characters will represent the user's initials and the four numeric characters will represent the user's last four digits of SS# or the month and day of birth (birth date). If no middle initial is given, letter "X" will be used.

#### Password

Password must be six (6) characters in length, alpha numeric in syntax, and in the format of AAAANN. The initial password, assigned by Help Desk, will expire at first sign on and system will prompt the user to create their individual unique password in this format.

### PROCEDURE FOR MEDITECH (Client Server sites)

#### Login ID

Same as MEDITECH MAGIC sites

#### Password

Essent Healthcare recognizes those facilities that are on the MEDITECH client server architecture can not force an alpha numeric format for passwords. For those facilities, passwords must be at least six (6) characters long and users must be encouraged to use an alpha numeric format.



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>Information Systems</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>User ID's and Passwords</b>	<b>Revision Date:</b>	<b>4/20/05</b>
<b>Policy #:</b>	<b>ISP-002</b>	<b>Review Date:</b>	<b>6/26/08</b>
<b>Responsible Party:</b>	<b>Chief Information Officer</b>	<b>Revision #:</b>	<b>2</b>

---

### **PROCEDURE FOR LOCAL AREA NETWORKS (Microsoft Active Directory)**

Essent Healthcare utilizes the Microsoft Active Directory as the primary method of authentication to the Essent network. A user is identified and authenticated with a Login ID and a Password. Below is the format for in which they are defined:

#### Login ID

Login ID must be in the following format: AAANNNN (Where AAA are the initials of the user and NNNN are the last four digits of the social security number)

#### Password

Passwords in the Active Directory must be at least six (6) characters in length.

### **Procedure for all other applications containing ePHI**

Each specific application will adhere to login ID and unique passwords setup as provided under the guidelines of the administrators of that application.

#### **References:**

HIPAA Section 164.308(a)(4)  
NIST Special Publication 800-12  
NIST Special Publication 800-53