



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to Information Systems	Revision Date:	6/26/08
Policy #:	ISP-001	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	3

Scope:

This policy is applicable to all employees, physicians, vendors, contractors, students, volunteers and any other person who is requesting electronic access to any Essent Healthcare, Inc. (“Essent”) information system, network, or application.

Purpose:

The purpose of this policy is to set forth guidelines for obtaining, modifying, or terminating a username and password in order to access information systems or applications that provide access to or house confidential or sensitive information.

Policy:

It is the policy of Essent to safeguard the confidentiality, integrity, and availability of all sensitive information contained within its information systems and applications by controlling access to those systems and applications. Access to all Essent systems is limited to only those individuals who are authorized to access those systems.

Authorization will be granted only upon completion and approval of Form ISF-001 “*Information Systems Access Request Form*”.

All workforce members are responsible for reporting incidents of unauthorized access to any system or application containing PHI or other sensitive information to their Facility Security Officer (FSO) immediately.

Definitions:

Sensitive information includes, but is not necessarily limited to, the following:

1. ***Protected Health Information (PHI)*** – Any individually identifiable health information that is created, maintained, stored, or transmitted by the facility.
2. ***Electronic Protected Health Information (ePHI)*** – PHI that is in electronic format.
3. ***Personnel files*** – Any information related to the hiring and/or employment of any individual who is or was employed by Essent Healthcare, Inc.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to Information Systems	Revision Date:	6/26/08
Policy #:	ISP-001	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	3

4. **Payroll data** – Any information related to the compensation of an individual during that individuals’ employment with Essent Healthcare, Inc.
5. **Financial/accounting records** – Any records related to the accounting practices or financial statements of Essent Healthcare, Inc.
6. **Other information that is confidential** – Any other information that is sensitive in nature or considered to be confidential or proprietary.

Workforce Member: (As defined by the HIPAA Regulations) includes employees, volunteers (board members, community representatives), trainees, students, contractors, and any other persons under the direct control of a covered entity.

I. Procedure for Establishing New User Access

Any individual requesting system access as a new user must complete and submit the Information System Access Request Form (Form # ISF-001). Be sure to check the “add new user” box at the top of the form. The completed form must be reviewed and signed by the employee’s immediate manager/supervisor and the FSO. Upon the approval, the form will be faxed to Essent Healthcare Help Desk at the Corporate Information Systems Department (CISD). All requests for new user access must be reviewed and approved by the corporate Chief Security Officer (CSO) or his/her designee. Form ISF-001 will be processed and entered into the system within 24 hours if received during normal business hours. Once the user account has been established, the CISD notify the FSO and department head. *Access will not be granted until a properly completed and authorized form ISF-001 (including a signed confidentiality statement) has been received by the CISD.* The CISD Help Desk shall retain the completed access request forms permanently.

For Department ‘owned’ applications such as Pro-Med, Kronos, and SSI, the user must indicate by either checking off the box provided for the specific application or by listing application under “other”. A copy of the form will be forwarded to the appropriate system’s access administrator(s) by the FSO. The access administrator will initial and date the form to indicate access has been provided. Once the account has been established, the new user will be contacted with his/her access information.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to Information Systems	Revision Date:	6/26/08
Policy #:	ISP-001	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	3

II. Procedure for Changing Existing User Access

Any existing user requesting a change to their system access must complete and submit the Information Systems Access Request Form (Form # ISF-001). Be sure to check the “modify existing user” box at the top of the form. The completed form must be reviewed and signed by the employee’s immediate manager/supervisor and the FSO. Upon the approval, the form will be faxed to CISD Help Desk. All requests for a change in access must be reviewed and approved by CSO or his/her designee. Changes will be made within 24 hours if received during normal business hours. Once the access change has been completed, the user will be notified by the CISD Help Desk.

III. Procedure for Termination of User Access

If an employee is terminated, or has accepted a new position within the facility that does not require computer access, the Human Resource department must notify the facility “Systems Access Group” by sending an e-mail within 24 hours. The user account will be inactivated immediately.

IV. Audit and Review Procedures

Each FSO is responsible for ensuring that user access is appropriate. Each FSO is responsible for completing an annual review of user access to ensure that system access is limited to only those individuals with a legitimate business need for the access.

References:

HIPAA Section 164.308(a)(4)
NIST Special Publication 800-12
NIST Special Publication 800-18
NIST Special Publication 800-53