



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Security	Revision Date:	4/21/05
Policy #:	ISP-008	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

Scope:

This policy applies to all workforce members of Essent Healthcare, Inc. (Essent).

Purpose:

The purpose of this policy is to define the appropriate security measures to be taken to protect workstations from unauthorized access, use, or disclosure.

Policy:

It is the policy of Essent to ensure that all workstations that are used to access, transmit, receive, or store sensitive information are appropriately secured so as to prevent unauthorized access, use, or disclosure.

Key Definitions

Workforce: (as defined in the HIPAA Regulations) Includes employees, volunteers (board members, community representatives), trainees, students, contractors, and other persons under the direct control of a covered entity.

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.

Procedures:

Note: Some of these measures may not be applicable to all types of workstations due to technological limitations. In such cases, all measures that are relevant to that workstation must be implemented.

1. All system administrator accounts must be password protected.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Security	Revision Date:	4/21/05
Policy #:	ISP-008	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

2. All users must logoff applications containing sensitive information before leaving their workstations. Where technologically feasible, auto logoff will occur after 60 minutes of inactivity.
3. Users are discouraged from storing data on the internal hard drive of the workstation instead of storing it on the network. All users are responsible for making backup copies of information stored on the internal hard drive of any workstation and for the security of such information. Data stored on internal hard drives will not be backed up by the CISD.
4. A user identification and password authentication mechanism must be implemented to control user access to the system.
5. All portable workstations (for example laptops) must be secured when not in use. Security may be provided by locking the equipment in a cabinet, desk, or office. Where such alternatives are not feasible, keeping the device out of sight in a desk or briefcase would be appropriate.
 - Keeping information that is stored on a portable computing device secure and current is the responsibility of the person who has the device in his/her possession and control. Those in possession are responsible for breaches of security related to devices in their possession.
6. A security patch and update procedure must be implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability being corrected.
7. A virus detection system must be implemented including a procedure to ensure that the virus detection software is properly maintained and up-to-date.
8. Workstations that are located in open, common, or otherwise insecure areas must also implement the following measures:
 - A password protected screen saver, inactivity timer, or automatic logoff mechanism must be implemented.
 - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.
9. All windows based workstations which access sensitive information are required to have either a password-protected screen saver or must be locked by the user when left unattended. Any exceptions must be approved in writing by the Chief Security Officer. In cases where password protected screen savers are not available, non-password protected screen savers should be enabled. The screen saver should activate after an inactivity period of 10 minutes maximum; users are free to activate their screen savers in fewer than 10 minutes if so desired.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Security	Revision Date:	4/21/05
Policy #:	ISP-008	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

10. All workforce members must have appropriate access authorization (user ID and password) prior to accessing any Essent workstation.
11. All computing devices owned by Essent shall be inventoried and tracked by the Information Systems Department in accordance with asset management, and device and media controls policies and procedures.
 - Permanent workstations (desktop computers, printers, and monitors) may only be moved by authorized IT workforce members or their designee.
 - All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by authorized IT workforce members or their designee.
12. All workforce members are required to monitor their workstations and report instances of unauthorized access to the Facility Security Officer immediately. Violations of this policy will result in sanctions up to and including termination of employment and/or civil or criminal prosecution.

References:

HIPAA Section 164.310(b) and (c)
NIST Special Publication 800-12
NIST Special Publication 800-14
NIST Special Publication 800-18
NIST Special Publication 800-53
CMS Information Security Acceptable Risk Safeguards (Version 1.1; April 7, 2004)