



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Use	Revision Date:	2/21/06
Policy #:	ISP-007	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Scope:

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

Purpose:

The purpose of this policy is to define the proper function, use, and physical attributes of the various end-user computing devices (“workstations”) found throughout the organization.

Policy:

It is the policy of Essent that all workstations are to be used exclusively for company business. Workforce members that use Essent information systems should have no expectation of privacy. To appropriately manage its information systems and enforce security measures, Essent may log, review, or monitor any data stored or transmitted on its information systems.

Key Definitions

Workforce: As defined in the HIPAA Privacy Rule, 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.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Use	Revision Date:	2/21/06
Policy #:	ISP-007	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Procedures:

1. The function of each workstation in the Essent computing enterprise is to provide a tool to facilitate the improvement of hospital operations and/or patient care.
2. Workstations are to be used only for official company business.
3. Workstations are to be used only by authorized individuals.
4. Each department is responsible for ensuring appropriate use of its workstations.
5. All workstations are monitored. Access audit logs will track failed login attempts, internet content filtering will track inappropriate use, and account audit logs will be used to verify user access rights.
6. Users are NOT to install their own software on any Essent workstation without prior approval from the FSO – this includes downloads from the internet or any other source.
7. Electronic mail should adhere to the same standards of conduct as any other form of mail. Respect those whom you contact electronically by avoiding distasteful, inflammatory or otherwise unacceptable comments. Email that contains harassing, embarrassing, sexually explicit, profane, obscene, intimidating, or defamatory information should be deleted by the user immediately. Likewise, materials that would offend someone on the basis of age, race, sex, sexual orientation, religion, political beliefs, national origin, or disability are strictly prohibited. Such materials should never be forwarded to others.
8. Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.
9. Distribution of excessive amounts of unsolicited mail is inappropriate.
10. While Essent encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material they find offensive or simply annoying.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Use	Revision Date:	2/21/06
Policy #:	ISP-007	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Guidelines

- **Be aware of the legal implications of your computer use.**
 - The Internet enables users to disseminate material worldwide. Thus the impact of dissemination on the internet is often far broader than that of a statement made on paper or in routine conversation. Keep in mind that a larger audience means a greater likelihood that someone may object with or without legal basis.
 - Much of what appears on the internet is protected by copyright law regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise and not copy or disseminate copyrighted material without permission. Copyright protection also applies to most software, which is often licensed to Essent with specific limitations on the number of users. Both individual users and Essent may, in some circumstances, be held legally responsible for violations of copyright laws.
 - Do not change the default settings on your workstation without prior approval from the FSO as these unapproved modifications may lead to security breaches.
 - The internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate information.
 - Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity apply to network-based communications.

- **Respect the mission of Essent and our responsibility to the community:**
 - Essent makes internet resources available to many of its workforce members to improve its operations and efficiencies. While incidental personal use is permissible in most settings, these resources are generally available only for official company business.
 - Remember that you are responsible for all activity involving your account. Keep your account secure and private. Do not use identifying data or common words as a password; your password should be difficult to crack or otherwise guess either by individuals or by sophisticated computer programs.
 - Essent is the custodian of a wide array of personal and financial data concerning its workforce members and patients, as well as the company itself. Respect Essent's



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Use	Revision Date:	2/21/06
Policy #:	ISP-007	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

obligations of confidentiality as well as your own. Only those with authorization may access, communicate or use confidential information.

- Material posted on WEB pages is generally accessible and thus deserves even greater thought and care than your private electronic mail. Remember that, absent restrictions, your web page is available to anyone, anywhere, and act accordingly.
- Essent has a right to expect that computer users will properly identify themselves at all times. Do not misrepresent yourself.

- **Do not harm the integrity of Essent's computer systems or networks.**
 - Today's information technology is a shared resource. Respect the needs of others when using computer and network resources. Do not tamper with equipment and avoid any actions that interfere with the normal operations of computers, networks, and facilities.
 - Avoid excessive use of computer resources. They are finite and others deserve their share. Chain mail, junk mail, and similar inappropriate uses of Essent resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to Essent's mission, may require Essent to ask that they be moved to a private internet service provider.
 - Although a respect for privacy is fundamental to Essent's policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that Essent must reserve the right to examine computer files, and that, in rare circumstances, Essent may be compelled by law or policy to examine even personal and confidential information maintained on Essent computing facilities.
 - You are granted privileges and responsibilities with your account. While these vary between workforce members, the use of Essent resources for personal commercial gain or for partisan political purposes is inappropriate and possibly illegal.
 - Individual Essent computer systems have varying resources and demands. Some have additional and sometimes more restrictive guidelines applicable to their own user. All workforce members are responsible for knowing and understanding the policies and procedures that pertain to any system to which they have access.

- **The Essent Code of Conduct applies to information technology as well as to other forms of communication and activity.**



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Workstation Use	Revision Date:	2/21/06
Policy #:	ISP-007	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

- Department managers or other individuals may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of Essent's information system.
 - Before any permanent action is taken against a user, the user will be advised of the bases for the proposed action and given an opportunity to respond. Concerns about such actions may be raised by contacting the Facility Security Officer.
 - Where a violation of Essent policies or applicable law appears to warrant action beyond a suspension or elimination of computer privileges, the matter will be referred to The Chief Security Officer and/or the Corporate Compliance Officer, or to law enforcement authorities.
 - Complaints or concerns about another's use of Essent computer resources should be directed to the Facility Security Officer, the Compliance Officer, or the compliance reporting hotline.
- Violations of this policy will lead to sanctions up to and including termination of employment and/or criminal or civil 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)