



ESSENT HEALTHCARE, INC.

Section:	Information Technology	Effective Date:	4/20/05
Subject:	Content Monitoring	Revision Date:	2/21/06
Policy #:	ISP-004	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 establish guidelines for the use of content filtering software to monitor electronic communications and to prevent objectionable and/or improper content from entering the information systems of Essent. Content filtering may also be used to prevent sensitive information from being transmitted over the system.

Policy:

It is the policy of Essent to utilize content filtering software to monitor electronic communications that occur on Essent information systems. Content filtering allows Essent to filter content from the internet, chat rooms, instant messaging, e-mail, e-mail attachments, and all other windows based applications. Use of any Essent system constitutes acceptance of this policy.

Essent strives to maintain a work environment that accommodates all of its workforce members. In this respect, Essent has implemented software to protect its workforce from unwanted exposure to offensive materials on the internet. When accessing the internet from any Essent workstation, employees are prohibited from accessing material that is harassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. All Essent workforce members are prohibited from accessing materials that would offend someone on the basis of race, age, sexual orientation, religion, political beliefs, national origin, or disability. Workforce members who encounter such material must immediately report the incident to their supervisor, the compliance reporting hotline, or the Compliance Officer.

Essent is not responsible for material viewed or downloaded from the internet. 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 material. Users accessing the internet do so at their own risk.



ESSENT HEALTHCARE, INC.

Section:	Information Technology	Effective Date:	4/20/05
Subject:	Content Monitoring	Revision Date:	2/21/06
Policy #:	ISP-004	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Procedures:

Users in Nashville TN, Haverhill MA, Ayer MA, Paris TX, Waltham MA, and Waynesburg PA are exposed to content filtering polices imposed by an iPrism 1200 appliance from St. Bernard Software at each respective location. Users in Sharon, CT are exposed to content filtering polices imposed by the Websense server running in Sharon – that contract ends in CY07 and will ultimately be replaced with an iPrism solution.

The iPrism devices are centrally managed by CIS in Waltham, MA with a policy set that blocks and logs access to inappropriate internet content. Reports may be generated on a schedule or on demand. The systems are configured to automatically update themselves on a daily basis.

Users may submit inaccessible URLs to icf@essenthealthcare.com that they need unblocked for business purposes only.

Where technologically feasible, the CIO will ensure that at network logon, the system shall display a message that informs the user that the system is only for use by properly authorized individuals; that system usage may be monitored, recorded, and/or audited; that unauthorized use is prohibited and subject to civil and/or criminal sanctions; and that use of the system indicates consent to monitoring.

References:

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