



ESSENT HEALTHCARE, INC.

Section:	Information Technology	Effective Date:	4/20/05
Subject:	Electronic Encryption	Revision Date:	10/10/06
Policy #:	ISP-016	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 encryption technology for email communications.

Policy:

Essent has implemented encryption technology within its email system to protect the privacy of sensitive information being transmitted outside of the organization. All emails that contain protected health information (PHI), or other sensitive information, must be encrypted before being sent outside of the organization.

Procedure:

E-mail may be used to send messages containing PHI within Essent Healthcare as long as the PHI used is limited to the minimum amount necessary. E-mails sent from one Essent employee to another are known as “internal communications” because they never leave Essent’s secure email system. Because they are secure, internal communications do not need to be encrypted.

Emails being sent to individuals outside of our organization are not considered to be secure because they are not constrained to the secure Essent system; they are transmitted via the internet. Therefore, *all messages that contain PHI or other sensitive information must be encrypted when being sent to individuals outside of our organization.*

There are two ways to encrypt a message as outlined in the attached user’s guide:

1. When composing an email that contains PHI, the user can use the “options” tab to set the sensitivity of the email to “confidential”. All confidential messages will be encrypted by the system.



ESSENT HEALTHCARE, INC.

Section:	Information Technology	Effective Date:	4/20/05
Subject:	Electronic Encryption	Revision Date:	10/10/06
Policy #:	ISP-016	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

2. When composing an email that contains PHI or other sensitive information, the sender can type the word “encrypt” into the subject line. All messages that contain the word “encrypt” anywhere in the subject line will be encrypted.

Please see the attached email user’s guide for more information on encrypting emails or contact the IT help desk for assistance.

References:

HIPAA Section 164.308(a)
NIST Publication 800-12
NIST Publication 800-18
NIST Publication 800-53
Essent Secure Email User’s Guide