Original Approval:	Effective:	Current Approval:	Next Review:
02/22/2010	03/05/2012	02/10/2016	02/10/2018

Business Partner Email Use Policy

Purpose

This policy is to ensure that standard practices are followed by ContinuUs associates and business partners that protect and safeguard protected health information when using electronic mail as a communication tool.

Cross-Reference

Email Use Policy
E-Mail Content
16 CFR Part 318, Health Breach Notification Rule; Final Rule - http://www.ftc.gov/os/2009/08/R911002hbn.pdf.

Definitions

ContinuUs associate – ContinuUs employee
Business partners - ContinuUs providers and staff, Third Party Administrator, System Contractors
PHI – protected health information
Email – Electronic Mail

Policy

1. **LEGAL RISKS**
   Email is a business communication tool and ContinuUs associates and business partners are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

   - If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and ContinuUs can be held liable.
   - If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and ContinuUs can be held liable.
   - If you unlawfully forward confidential information, you and ContinuUs can be held liable.
   - If you send an attachment that contains a virus, you and ContinuUs can be held liable.

   By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and ContinuUs will disassociate itself from the user as far as legally possible.

2. **LEGAL REQUIREMENTS**
   The following rules are required by law and are to be strictly adhered to:

a. It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
b. Do not send unsolicited email messages.
c. Do not forge or attempt to forge email messages.
d. Do not send email messages using another person's email account.
e. Do not disguise or attempt to disguise your identity when sending email.

3. BEST PRACTICES

ContinuUs considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. ContinuUs associates and business partners shall adhere to the following guideline:

Email Content:

- Password protect all attachments that contain confidential information.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).

4. CONFIDENTIAL INFORMATION

Some email systems have built in security between the email client, server and transport layer. ContinuUs' email system has this built in security. There is no assurance that all ContinuUs business partners have an acceptable security level built into their email communications. To protect email communications containing confidential information ContinuUs associates and business partners shall take extra steps in security.

- Do not use any personal identification information within the subject line or body of an email message. This includes but is not limited to social security number, full member name, Medicaid (pre MCI) or Medicare numbers, combination of address and full member name.
- Password protect all attachment files that contain protected health information or confidential business data.
- Do not send password in the same email that contains the password protected file.
- Use a generic number, such as a member's MCI number in the body of an email if you need to make a reference to a specific member.

5. SYSTEM MONITORING

You must have no expectation of privacy in anything you send to or receive from an ContinuUs email address. Emails to ContinuUs shall be monitored without prior notification to verify compliance with confidentiality regulations. If there is evidence that you are willingly and repetitively sending protected health information by not adhering to the guidelines set out in this policy, ContinuUs is required to disclose the information to proper authorities based on the Health Breach Notification Rule.

Procedure

1. Refer to Email Use and Email Content policies.

History

3/21/11 – Updated procedure to refer to IT.2.4 policy. Confidential Information – added pre MCI verbiage. Prior to MCI numbers the Medicaid number was a members social security number with 0. Added policy information in cross-reference section.

3/5/12 – Presented to Operations Team for final approval.