	PCHP.PV.106 Emailing Protected Health Information V3 PCHP.PV.106	
CENTRA	Name:	PCHP.PV.106 Emailing Protected Health Information
	ID Number:	PCHP.PV.106
	Approval Date:	01/30/2018 09:55:31 AM
	Approved By:	Garland Morton/CentraNotes

Body

Policy Name: Emailing Protected Health Information

Scope: Entire Piedmont workforce

Purpose: To ensure the appropriate use of email systems when transmitting Protected Health Information (PHI).

Definitions & Acronyms:

CMS: Centers for Medicare & Medicaid
CFR: Code of Federal Regulations
PBM: Pharmacy Benefit Manager
HIPAA: Health Insurance Portability and Accountability Act of 1996
HITECH: Health Information Technology for Economic and Clinical Health Act
PHI: Protected Health Information

Piedmont: "Piedmont" collectively refers to Piedmont Community Health Plan (PCHP), Piedmont Community HealthCare (PCHC) and any future entities that are owned, affiliated with and/or operated by Piedmont.

Policy:

1. Piedmont must protect the electronic transmission of PHI through emails.
2. Piedmont will only release the minimum necessary to meet the requestor's needs.
3. Whenever appropriate, Piedmont will de-identify information that will be used.
4. When sending emails containing PHI to external recipients outside Centra's network, Piedmont will send by secured email.
5. Piedmont will implement security measures to ensure electronically transmitted ePHI cannot be improperly modified without detection until disposed.
6. Piedmont will implement encryption mechanisms to encrypt ePHI when deemed appropriate.

Procedures:

1. All employees are set up with a unique identity complete with unique password and file access controls. Passwords must be changed every 90 days.
2. Employees will restrict their use of email for communicating normal business information such as information about general care and treatment of members, operational and administrative matters.
3. Email users should verify the accuracy of the email address before sending any PHI, and if possible, use email addresses loaded in the system address book.
4. PHI may be sent unprotected via email within the properly secured, internal network provided by Centra (i.e., employee to employee through Microsoft Outlook).
5. When emailing PHI outside of the Piedmont internal network, always send it securely.

A. Type [Secure] at the beginning of the subject line followed by the Subject matter.

B. DO NOT include PHI in the Subject line.

C. Centra's network will capture the [Secure] request and send an encrypted version of the email out to the recipient.

D. Centra's network performs routine scanning of content in emails for PHI. If PHI is identified in the subject or body of an email, Centra's network will automatically encrypt and send secured.

6. All email containing PHI must contain Piedmont's email confidentiality notice as stated here:

> **Confidentiality Notice:** This email transmission may contain confidential health information or other information that is privileged and/or confidential and which may be subject to legal restrictions and penalties regarding its unauthorized disclosure or other use. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this e-mail is strictly prohibited. If you have received this e-mail transmission in error, please reply to the sender, so that arrangements can be made for proper delivery, and then please permanently delete the e-mail (and all attachments) from your e-mail and computer systems.

7. Employee email access privileges will be removed promptly following their departure from employment with Piedmont, see PCHP.PV.105 for additional access removal procedures.

8. Email messages, regardless of content, should not be considered secure and private. The amount of information in any email will be limited to the minimum necessary to meet the needs of the recipient.

9. Piedmont relies on Centra's network for implementation of security measures to ensure ePHI cannot be improperly modified without detection.

10. Employees should immediately report any violation of this guideline to their Supervisor, Compliance Officer, or the Compliance Department.

Equipment: None

Forms and Letters: None

Reference(s): 45 CFR § 164.312(e) – Security Standards for the Protection of Electronic PHI -

Interdisciplinary Review: None

Policy History:

Date	Revision No.	Reason for Change	Sections Affected
04/14/2003	NEW		All
09/23/2013	1.0	• Updated policy to new format. • Provided more detailed clarification.	All
02/01/2016	1.1	• Converted to Centra Format	
07/05/2016	2.0	• Reviewed for compliance with phase 2 audit protocol • Amended network information and removed some stale information regarding transmission of SECURE emails. • Added Centra to procedure 4, 5B	procedure 4, 5B, 7
01/24/2018	3.0	• Reviewed for compliance with HIPAA Audit Protocol • Added Secure submission policy (HAP#143)	Policy #4, 5, 6

		• Added security policy regarding improper modification (HAP#144) • Added security encryption language (HAP#145)	

Document Link Manager

No Documents Linked No Documents Linked

Attachment Manager

No Attachments