HIPAA/PRIVACY

Emailing Protected Health Information

Patient Name:LASTNAME, FIRSTNAME **Date:08-Apr-2019**

PURPOSE

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

POLICY

It is the policy of this Facility to protect the electronic transmission of PHI as well as to fulfill our duty to protect the confidentiality and integrity of patient PHI as required by law, professional ethics and accreditation requirements. The information released will be limited to the minimum necessary to meet the requestor's needs. Whenever possible, de-identified information will be used.

PROCEDURE

1) E-mail users will be set up with a unique identity complete with unique password and file access controls.
2) E-mail users may not intercept, disclose or assist in intercepting and disclosing e-mail communications.
3) Patient specific information regarding highly sensitive health information must not be sent via e-mail, even within the internal email system (i.e. information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
4) Users will restrict their use of email for communicating normal business information such as information about general care and treatment of patients, operational and administrative matters, such as billing.
5) 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.
6) PHI may be sent unprotected via e-mail within a properly secured, internal network of the organization. When sending PHI outside of this network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information. Sample security measures include password protecting the document(s) being sent or encrypting the message.
7) All e-mail containing PHI will contain a confidentiality statement (see sample below).
8) Users should exercise extreme caution when forwarding messages. Sensitive information, including patient information, must not be forwarded to any party outside the organization without using the same security safeguards as specified above.

9) Users should periodically purge e-mail messages that are no longer needed for business purposes, per the organization's records retention policy.

10) Employee e-mail access privileges will be removed promptly following their departure from the organization.

11) 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.

12) Employees should immediately report any violations of this guideline to their supervisor, Administrator or Facility Privacy Official.

Patient or Representative's Signature

Date: 08-Apr-2019

Print Name Lastname, Firstname

Representative's Relationship to Patient Self

Submit