


|  |  |                            |                             |                     |
|--|--|----------------------------|-----------------------------|---------------------|
|  <p>Heritage<br/>Provider Network<br/>&amp;<br/>Affiliated Medical Groups</p> | Program: HIPAA Compliance                |                            |                             |                     |
|  | Policy No.                               | Effective Date: 01/01/2012 | Page - 1 -                  |                     |
|  | Authored by:<br>Compliance Sub Committee | Date:<br>01/01/2012        | Revised by:<br>Sandy Finley | Date:<br>02/02/2015 |
|  | Approved by:<br>Compliance Committee     | Date:<br>02/02/2015        |                             |                     |
| Title of Policy: HIPAA Compliance as it Relates to Email and Electronic Data Transmission  |  |                            |                             |                     |

**PURPOSE:**

The Electronic Data Transmission (EDT) policy has been developed to reflect Heritage Provider Network and its Affiliated Medical Groups’ (HPN) business practices as it pertains to appropriately utilizing and safeguarding ePHI, as required by HIPAA, HITECH Act, federal and state regulations, and health plan requirements. As employed or contracted with the company, all employees and Business Associates enter into agreement to abide by this policy, and/or as set forth in the terms outlined in the Business Associate Agreements.

**POLICY:**

“Electronic Data Transmission Resources” refers to HPNs’ PCs, portable/laptop PCs, handheld PCs, servers, network connections, process control computers, modems, cable, all telephone equipment, all software and program applications and related hardware and equipment, and all electronic communication systems such as telephones, cell phones, pagers, e-mail, voice-mail, facsimile (fax), and the Intranet or Internet.

HPN will implement a process by which all electronic communication transmitted outside of the organization will be properly encrypted. Company encourages every organization to use an encryption service.

Text messaging via any device is strictly prohibited as the text cannot be password protected or encrypted.

**RESPONSIBILITY:**

Corporate Security Officer, Director of MIS, Director of Human Resources, Compliance Officer and Corporate Compliance Officer

**PROCEDURE:**

1. The company designates upon approval the ability/permission to create, receive, maintain and transmit ePHI in accordance to the needs of the company and as it pertains to the role, duty, and responsibility of the transmitter (e.g. employee, Business Associate, vendor, etc.).
2. In an effort to appropriately safeguard ePHI, the company determines these permissions based on the necessity to perform essential job duties and the ability to appropriately safeguard the transmission of ePHI as outlined in this policy.



Heritage  
Provider Network  
&  
Affiliated Medical Groups

|  |                            |                             |                     |
|--|----------------------------|-----------------------------|---------------------|
| Program: HIPAA Compliance                |                            |                             |                     |
| Policy No.                               | Effective Date: 01/01/2012 |                             | Page - 2 -          |
| Authored by:<br>Compliance Sub Committee | Date:<br>01/01/2012        | Revised by:<br>Sandy Finley | Date:<br>02/02/2015 |
| Approved by:<br>Compliance Committee     | Date:<br>02/02/2015        |                             |                     |


Title of Policy: HIPAA Compliance as it Relates to Email and Electronic Data Transmission

3. Failure to comply with this policy may result in disciplinary action for employees, up to and including termination of employment.
4. Specific Business Associate use/restrictions and confidentiality agreements will be identified on individual contracts. Any use, other than intended, may result in termination of individual contracts.
5. Legal action will be considered as identified depending upon the severity of circumstances related to policy non-compliance.
6. The company’s e-mail system must not be used for the purpose of communicating patient identifiable health information (PHI) at any time, unless the file is encrypted. This includes e-mails sent inter-company and e-mails sent outside the company.
5. In general, confidential information should not be e-mailed regardless if it contains PHI. This will ensure privacy and confidentiality of all confidential material and information.
6. On rare occasions, if an employee is required to send ePHI via e-mail, he or she must contact Management Information Systems so they can be set up with appropriate encryption tools. No exceptions.

Compliance:

- a. HPN’s Electronic Data Transmission policy complies with applicable state and federal laws and regulations, and health plan regulations.
- b. Strict patient privacy and confidentiality measures will be applied to all electronic transfers involving patient information, records and personal data.
- c. Accessing, sending, forwarding, requesting or facilitating the receipt or transmittal of Electronic Protected Health Information (ePHI) by e-mail that is not encrypted is a violation of company policy. Employees who receive or send ePHI must obtain authorization from the Director of MIS to insure appropriate safeguards have been established.
- d. All outgoing e-mails must contain the following verbiage regarding confidentiality:

**IMPORTANT WARNING:** This e-mail is intended for the use of the person to whom it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this e-mail is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this

|  |  |                            |                             |                     |
|--|--|----------------------------|-----------------------------|---------------------|
|  <p>Heritage<br/>Provider Network<br/>&amp;<br/>Affiliated Medical Groups</p> | Program: HIPAA Compliance                |                            |                             |                     |
|  | Policy No.                               | Effective Date: 01/01/2012 | Page - 3 -                  |                     |
|  | Authored by:<br>Compliance Sub Committee | Date:<br>01/01/2012        | Revised by:<br>Sandy Finley | Date:<br>02/02/2015 |
|  | Approved by:<br>Compliance Committee     | Date:<br>02/02/2015        |                             |                     |
| Title of Policy: HIPAA Compliance as it Relates to Email and Electronic Data Transmission  |  |                            |                             |                     |

information is **STRICTLY PROHIBITED**. If you have received this message in error, please notify us immediately and delete the related e-mail.

**Monitoring:**

The use of HPN’s EDT is a privilege. Individual privileges may be revoked or restricted by the company at any time.

- a. HPN reserves the right to monitor (without prior notice) any EDT resources at random or at the discretion of managers/supervisors and/or administration. Telephone and facsimile activity will be monitored monthly by Administration and department managers/supervisors.
- b. All information including data and communications stored in or transmitted by or through any HPN electronic transmission system will be regarded as confidential and proprietary.
- c. The Corporate Security Officer will monitor policy changes/updates.
- d. The Director of Quality Management will monitor patient data policies and updates as identified by Health Plan/Accreditation requirements.
- e. Any breach of this policy, by any employee or contractor, will be reported immediately to the Director of Human Resources and Compliance Officer.


**Hardware/Software:**

- a. Hardware: The MIS department is solely authorized to connect or integrate hardware and equipment. Any form of personal unauthorized hardware modification by any employee is strictly prohibited. Unauthorized hardware connection may result in hardware being removed or disabled, under the direction of Administration, without prior notice.
- b. Software: The MIS department is responsible to authorize and install all software. The MIS department, under the direction of Administration, may delete or disable any unauthorized software or program application without prior notice.
- c. The unauthorized access, use, copying, distribution or unintended use, in whole or in part, of HPN’s proprietary software is strictly prohibited.

**Security Measures:**

**Patient Security**

- a. The Corporate Security Officer is designated as the official responsible to monitor policies related to all EDT resources in regard to all “Patient’s Right to Privacy” policies.

|  |  |                            |                             |                     |
|--|--|----------------------------|-----------------------------|---------------------|
|  <p>Heritage<br/>Provider Network<br/>&amp;<br/>Affiliated Medical Groups</p> | Program: HIPAA Compliance                |                            |                             |                     |
|  | Policy No.                               | Effective Date: 01/01/2012 | Page - 4 -                  |                     |
|  | Authored by:<br>Compliance Sub Committee | Date:<br>01/01/2012        | Revised by:<br>Sandy Finley | Date:<br>02/02/2015 |
|  | Approved by:<br>Compliance Committee     | Date:<br>02/02/2015        |                             |                     |
| Title of Policy: HIPAA Compliance as it Relates to Email and Electronic Data Transmission  |  |                            |                             |                     |

- b. HPN’s Internet sites have the Privacy Policies, including HIPAA required privacy notice, posted on the web page for patient access. Additional patient material and mailings are generated through the Marketing Department in an effort to disclose the company’s privacy protection practices.
- c. See other related policies and procedures related to HIPAA security located on the company’s website under HIPAA Security Rule.

Employee Security

- a. The MIS department is responsible to assign and enforce employee identification passwords and accountability. Utilizing or allowing the use of an unassigned password in an attempt to access patient and/or company information (restricted or otherwise) is strictly prohibited.
- b. The removal of any EDT from company premises, without written documentation and/or permission from MIS and/or Administration is strictly prohibited.
- c. The MIS department is responsible to ensure all patient data and HPN’s documents are protected during the disposal, selling and/or re-issuing of any company EDT system.
- d. The MIS Department will ensure adequate and secured disaster recovery policies for all patient and company data.

REFERENCE: 45 CFR § 164.530(c)