HealthLX External Transmission Policy

Last Updated: 2/01/2025

© 2025 HealthLX, LLC | CONFIDENTIAL & PROPRIETARY

Table of contents

Overview

It is the policy of HealthLX to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. As such, this policy outlines the requirements for transmission of electronic protected health information (ePHI) to ensure the security and integrity of such ePHI.

Policy

ePHI transmissions to non-HealthLX entities

1. To appropriately guard against unauthorized access to or modification of ePHI that is being transmitted from HealthLX networks, the following procedures outlined must be implemented:
    a. All transmissions of ePHI from HealthLX must utilize encryption between the sending and receiving entities of the file, document, or folder containing said ePHI before transmission.
    b. Prior to transmitting ePHI the receiving person or entity must be authenticated.
    c. All transmissions of ePHI should include only the minimum amount of PHI.

ePHI transmissions using electronic removable media

1. Removable media includes:
    a. Floppy disks
    b. CDROM
    c. Memory cards
    d. Magnetic tape
    e. Removable hard drives
    f. USB/Flash drives
2. When using removable media, the sending party must:
    a. Use encryption to protect against unauthorized access or modification.

© 2025 HealthLX, LLC | CONFIDENTIAL & PROPRIETARY

    b. Authenticate the person or entity requesting said ePHI in accordance with HealthLX Policies.
    c. Send the minimum amount necessary to the receiving person or entity.

3. If using removable media for the purpose of system backups and disaster recovery and the removable media is stored and transported in a secured environment, no additional security mechanisms are required.

ePHI transmissions using email or messaging systems

1. For more information regarding email use, view the Internet and email Use Policy.
2. The transmission of ePHI via an email or messaging system to a patient is permitted if the sender has ensured that the following conditions are met:
   a. The individual has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.
   b. The individual has provided written authorization to HealthLX to utilize an email or messaging system to transmit ePHI to them.
   c. The individual's identity has been authenticated.
   d. The email or message contains no excessive history or attachments.
3. The transmission of ePHI to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:
   a. The receiving entity has been authenticated.
   b. The receiving entity is aware of the transmission and is ready to receive said transmission.
   c. The sender and receiver are able to implement a compatible encryption mechanism.
   d. No ePHI is contained in the non-encrypted areas of the communication.
   e. All attachments containing ePHI are encrypted.
   f. Email accounts that are used to send or receive ePHI must not be forwarded.

ePHI transmissions using wireless LANs and devices

1. The transmission of ePHI over a wireless network within the HealthLX networks is permitted if the following conditions are met:
   a. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
   b. The local wireless network is utilizing an encryption mechanism for all transmissions over the wireless network.
2. If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.
3. The authentication and encryption security mechanisms implemented on wireless networks within the networks are only effective within those networks.
4. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

Additional requirements for electronic transmissions

1. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 256-bit encryption. (See Encryption and Authentication Suggestions)
2. When transmitting ePHI electronically, regardless of the transmission system being used, users must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the ePHI requested.

3. If the ePHI being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PHI should be transmitted.

Violations:

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
2. Violation may also result in civil and criminal penalties to HealthLX as determined by federal and state laws and regulations related to loss of data.