[Insert Company Name and Logo]	
Title: Electronic Information Transmission Security	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy outlines the requirements for transmission of sensitive and regulated data to ensure the security and integrity of such sensitive and regulated data.

Scope: This policy applies to all employees and other workforce members (whether paid, volunteer or contractor) working in all facilities under the organization's ownership.

Procedure:

1. To appropriately guard against unauthorized access to or modification of sensitive and regulated data that is being transmitted from [Insert Company name] networks, the following procedures outlined must be implemented:
    i. All transmissions of sensitive and regulated data from [Insert Company name] must utilize encryption between the sending and receiving entities of the file, document, or folder containing said sensitive and regulated data before transmission.
    ii. Prior to transmitting sensitive and regulated data the receiving person or entity must be authenticated.
    iii. All transmissions of sensitive and regulated data should include only the minimum amount of PHI.
2. Removable media includes:
    i. Floppy disks
    ii. CDROM
    iii. Memory cards
    iv. Magnetic tape
    v. Removable hard drives
    vi. USB/Flash drives
    b. When using removable media, the sending party must:
        i. Use encryption to protect against unauthorized access or modification.
        ii. Authenticate the person or entity requesting said sensitive and regulated data in accordance with [Insert Company name] Policies.
        iii. Send the minimum amount necessary to the receiving person or entity.
    c. 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.
3. Sensitive and regulated data transmissions using email or messaging systems

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

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

4. Sensitive and regulated data transmissions using wireless LANs and devices
    a. The transmission of sensitive and regulated data over a wireless network within the [Insert Company name] networks is permitted if the following conditions are met:
        i. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.
        ii. The local wireless network is utilizing an encryption mechanism for all transmissions over the wireless network.
    b. If transmitting sensitive and regulated data over a wireless network that is not utilizing an authentication and encryption mechanism, the sensitive and regulated data must be encrypted before transmission.
    c. The authentication and encryption security mechanisms implemented on wireless networks within the networks are only effective within those networks.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

d. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

5. Additional requirements for electronic transmissions
    a. 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)
    b. When transmitting sensitive and regulated data 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 sensitive and regulated data requested.
    c. If the sensitive and regulated data 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:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.