	Information Security Policies and Procedures	No. COMP-Sec 8.3.6
	Title: TRANSMISSION SECURITY PROCEDURE	Page: 1 of 4
		Revised Date: 12/22/04
		Original Date: 12/22/04

Transmission Security Procedure

I. SCOPE

This procedure applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This procedure applies to all Tenet information assets and information asset Administrators.

II. PURPOSE

Provide guidelines for the implementation of safeguards for *CONFIDENTIAL* information that is being transmitted over an electronic communications network. The transmission of data from Tenet information assets should be protected against unauthorized access and modification.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. PROCEDURE

Transmissions from Tenet information assets shall be secured to ensure that data is not accessed or modified by unauthorized users. Administrators and users of Tenet information assets shall use only secure methods when transmitting *CONFIDENTIAL* information.

A. Transmissions Via Email


Email is only considered to be a secure transmission method when the email is transmitted wholly between Tenet email addresses, or the email and its attachments are encrypted.

1. TENET EMAIL

Emails transmitted from a tenethealth.com (or other Tenet managed email) address to one or more tenethealth.com (or other Tenet managed email) addresses, and no outside email addresses, are considered to be secure transmissions.

2. EXTERNAL EMAIL

Emails transmitted from a tenethealth.com (or other Tenet managed email) address to one or more non-Tenet email addresses are only to be considered secure transmissions if the following procedures are followed:

	Information Security Policies and Procedures	No. COMP-Sec 8.3.6
	Title: TRANSMISSION SECURITY PROCEDURE	Page: 2 of 4
		Revised Date: 12/22/04
		Original Date: 12/22/04

- a) If the email subject contains *CONFIDENTIAL* information, the email shall not be transmitted to any non-Tenet email addresses.
- b) If the email body contains *CONFIDENTIAL* information, the email transmission should be secured by using the Email Encryption method in accordance with Encryption Control Procedure No. 8.1.3.
- c) If the email body and an attachment contain *CONFIDENTIAL* information, the email transmission should be secured by using the Email Encryption method in accordance with Encryption Control Procedure No. 8.1.3.
- d) If the email body does not contain *CONFIDENTIAL* information, but at least one attachment does, the email transmission should be secured by using the Email Encryption method in accordance with Encryption Control Procedure No. 8.1.3. Alternatively, the email may be sent without encryption, with the attachment protected using the Data Encryption method outlined in Encryption Control Procedure No. 8.1.3. In this case, the password or decryption key should be distributed to the recipient in a separate email, or preferably through a different means of communication.

B. Transmissions within the Tenet Trusted Network


Transmissions where the originating point, the receiving point, and all network paths traveled are inside a Tenet trusted network are considered to be secure transmissions. The Tenet trusted network is defined in Network Connections Procedure No. 8.3.3.

C. Transmissions outside the Trusted Network

Transmissions where the originating point, the receiving point, and/or at least one network path traveled is outside a Tenet trusted network are only to be considered secure when appropriate safeguards are implemented to secure the transmission. If the transmission method is not secure, then the *CONFIDENTIAL* data should be secured by using Data Encryption in accordance with Encryption Control Procedure No. 8.1.3. In this case, the password or decryption key should be distributed to the recipient in a separate email, or preferably through separate means of communication.

1. DEDICATED CIRCUITS

Dedicated circuits between a Tenet trusted network and a third party are considered to be secure transmission methods.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.6
	Title: TRANSMISSION SECURITY PROCEDURE	Page: 3 of 4
		Revised Date: 12/22/04
		Original Date: 12/22/04

2. TUNNEL CONNECTIONS

VPN and other tunnel connections between a Tenet trusted network and a third party are considered to be secure transmission methods. These connections must be configured in accordance with Network Connections Procedure No. 8.3.3 and Encryption Control Procedure No. 8.1.3.

3. SECURE FILE TRANSFER METHODS

The transmission may be considered secure if a secure file transfer method (i.e. HTTPS, SFTP) is used and user authentication complies with UserID Control Procedure No. 8.1.1 and Password Control Procedure No. 8.1.2.

4. DIAL-UP CONNECTIONS

Dial-up connections should only be considered secure transmission methods if the *CONFIDENTIAL* information is traveling using another secure transmission method noted above.


D. Wireless Transmissions

Wireless connections include Wireless Local Area Networks (WLANs) and any other wireless devices that may send or receive Tenet *CONFIDENTIAL* information. This policy generally deals with WLAN technology, but the principles shall be applied to any wireless technology. Wireless connections are considered secure when established in accordance with Network Connections Procedure No. 8.3.3 and Encryption Control Procedure No. 8.1.3.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0 and its subordinate Standards and Procedures.
- Security Risk Management Standard No. 7.1.0.
- Asset Access Controls Standard No. 8.1.0 and its subordinate Procedures.
- Encryption Control Procedure No. 8.1.3.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.6
	Title: TRANSMISSION SECURITY PROCEDURE	Page: 4 of 4
		Revised Date: 12/22/04
		Original Date: 12/22/04

- Logging and Auditing Procedure No. 8.2.2.
- Network Security Administration Standard No. 8.3.0.
- Network Security Administration Procedure No. 8.3.1.
- Network Access Controls Administration Procedure No. 8.3.2
- Network Connections Procedure No. 8.3.3.
- Tenet Administrative Policies and Procedures No. 2.18 “Coordination of Information Processing Systems”.