	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 1 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

Information Handling 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 Users.

II. PURPOSE

Provide a procedure for handling information assets containing *CONFIDENTIAL* or *PROPRIETARY* information. Information is subject to misuse, loss, theft, and unauthorized revision during any of the steps involved in handling or processing. Procedures for handling are needed to assist in protecting the information while it is in possession of the corporation.

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 Controls Exception Book.


III. PROCEDURE

When information of various sensitivity classifications is combined, the resulting collection of information shall be assigned the most restrictive sensitivity level found anywhere in the information.

1. Workstation Use

A workstation is any point of access to Tenet’s information assets including, without limitation, computer terminals, personal computers, laptops, and hand held computing devices.

- a) In a shared environment, where a computing resource is used by more than one individual (such as a nursing station), Users shall exit from any applications where their personal UserID and password were applied before leaving the workstation.
- b) In a non-shared environment (such as an office setting), Users shall apply a password protected screen saver.
- c) At the end of each work shift, Users shall lock or log off of their workstations so as to restrict access to that workstation to only authorized Users.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 2 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- d) All workstations, terminals or other monitors shall be equipped with automatic logoff or a password required screen saver.
 - (i) The automatic log off function shall be set appropriately for the workstation environment, but it is strongly recommended that automatic logoff occur after fifteen (15) minutes of inactivity.
 - (ii) The password-protected screen saver, if used, shall be set to activate after an inactivity period appropriate for the environment. It is strongly recommended that the screen-saver activate after fifteen (15) minutes of inactivity, but the exact time settings should be determined by facility management.
 - (iii) It is recommended that a shortcut or icon be provided to allow for the instantaneous application of the password-protected screen saver.
 - (iv) The password function shall be active and conform to the Password Use Procedure Number 3.3.2.


2. Dissemination by Classification

Information may be transmitted in a variety of formats, including electronic (e-mail, File Transfer Protocol, Electronic Data Interchange), hard copy, or other media, and shall always be accomplished in accordance with the policies appropriate to the classification level of the data.

- a) *CONFIDENTIAL* - Dissemination of this information shall be limited to individuals who have a “need to know”.
- b) *PROPRIETARY* - Dissemination of this information is on an as needed basis for Tenet information asset Users.

3. Dissemination to Third Parties

A Business Associate may create, receive, maintain, or transmit information assets on Tenet’s behalf only if the Business Associate has given Tenet satisfactory assurances, as evidenced by a written contract, that the Business Associate will appropriately safeguard such Information Assets. The written contract must comply with Tenet Privacy Policies & Procedures No. 1.1.1 “Contracts with Business Associates” and provide that the Business Associate will:

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 3 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- a) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Information Assets that it creates, receives, maintains, or transmits on behalf of Tenet;
- b) Ensure that any agent, including a subcontractor, to whom it provides such information assets agrees to implement reasonable and appropriate safeguards to protect it;
- c) Report to Tenet any security incidents of which it becomes aware; and
- d) Authorize termination of the contract by Tenet if Tenet in its sole discretion determines that the Business Associate has violated a material term of the contract.


Once aware of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangement, Tenet must take reasonable steps to cure the breach or end the violation. If such steps are not successful, Tenet must terminate the contract or arrangement; provided, however, that if termination is not feasible, Tenet will report the problem to the Secretary of the U.S. Department of Health & Human Services.

All disclosures of *CONFIDENTIAL* or *PROPRIETARY* Tenet information to third parties, outside a Business Associate agreement, shall be accompanied by a signed Confidentiality and Non-Disclosure Agreement (See Addendum A). This approach is not an alternative to establishing a Business Associate agreement with a third party and shall only be used in emergencies or special situations.

4. Receipt of Third Party Information

These directions apply to information not created by Tenet and obtained from a third party.

- a) Information obtained from a third party shall be assigned an appropriate classification on behalf of the third party by the Information Owner. Unless more restrictive security measures are specified otherwise by contract, all information that has been entrusted to Tenet by a third party shall be protected at the equivalent Tenet information level, *CONFIDENTIAL*, *PROPRIETARY*, or *PUBLIC*.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 4 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- b) Users shall not sign confidentiality agreements provided by third parties without the advance authorization of Tenet’s legal counsel designated to handle intellectual property matters.
- c) To prevent inadvertent disclosure of Tenet information, when a third party provides Tenet with information on computer media (tapes, disks, CD-ROMs, etc.) and requests the media be returned, Tenet staff shall instead provide the external entity with written assurance that the media has been destroyed. If destruction of the computer media is not feasible, Tenet shall ensure and certify in writing that any *CONFIDENTIAL* and/or *PROPRIETARY* information is removed from the computer media before returning it to a third party.

5. Computer Storage Media Requirements

When using storage media (tapes, floppies, etc.) to send information to a third party, an inadvertent disclosure of previously recorded information shall be avoided. All computer storage media being sent to a third party shall be:

- a) Unused media, or
- b) Cleansed using a zeroization or degaussing process in accordance with approved procedures (See the Tenet Administrative Management Policies and Procedures No. 1.11 “Records Management” for further information), and then reformatted before being used.


6. Data Requests from Outside Sources

Refer to Administrative Policy and Procedure No. 1.9, “Public Release of Information” for further information.

A. HANDLING CONFIDENTIAL AND PROPRIETARY INFORMATION

Protected health information records shall receive special handling. All handling instructions in this section apply. In addition, refer to the Administrative Policies and Procedures No. 1.10 “Access to Patient and Medical/Professional Staff Records.”

The following items provide guidelines for Users of Tenet *CONFIDENTIAL* and *PROPRIETARY* information that shall assist in protecting the confidentiality, availability, and integrity of this information.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 5 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

1. Inadvertent Viewing of Information


Unauthorized individuals may inadvertently view *CONFIDENTIAL* and *PROPRIETARY* information simply by looking at material on a desk or nurses station, or by looking at a computer screen. If an individual inadvertently views protected health information, this disclosure may need to be tracked in the Disclosure Tracking Application or a similar tool; please see Privacy Policy and Procedures No. 1.3.4 for details. The following safeguards shall be implemented to prevent these disclosures:

- a) Screens on information assets that display *CONFIDENTIAL* and *PROPRIETARY* information shall not be legibly visible from outside the immediate work area. They shall be positioned to restrict viewing from hallways, reception areas, waiting rooms, and other public areas, and/or a filter restricting the angle for viewing a screen may be employed.
- b) If an unauthorized person enters an area where *CONFIDENTIAL* and *PROPRIETARY* information is present, steps to conceal the information shall immediately be taken.
 - (i) Information on paper documents can be covered with other material or one-sided documents can be turned over to face down.
 - (ii) Information displayed on a computer screen shall be covered by a password-protected screen saver or the User shall log-off. It is recommended that this password-protected screen saver activate after fifteen (15) minutes of inactivity, but the exact time settings should be determined by facility management.
- c) At the end of the work shift, users shall make reasonable efforts to secure *CONFIDENTIAL* and *PROPRIETARY* information, including locking office doors, drawers and filing cabinets where possible.

2. Copying and Printing Information

Making additional copies or printing extra copies of *CONFIDENTIAL* information should only be conducted when necessary.

- a) Users shall not leave the machine unattended during the copying process. The machine should be attended until the originals and all copies of the *CONFIDENTIAL* information are removed from the machine.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 6 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- b) *CONFIDENTIAL* output shall be delivered directly to the designated recipients. Such output shall never be delivered to unsecured locations, such as unattended desks or unoccupied offices.
- c) If a copy machine, printer, or other reproduction machine jams or malfunctions, Users shall not leave the machine until all copies of *CONFIDENTIAL* information are removed.
- d) Waste copies of *CONFIDENTIAL* information generated in the course of copying, printing, or otherwise handling such information shall be destroyed according to approved procedures (See the Tenet Records Management Policy and Procedure No. 1.11 for further information).


Reproduction of *PROPRIETARY* information should be authorized as needed.

- a) Users shall not leave the machine unattended during the copying process. The machine should be attended until the originals and all copies of the information are removed from the machine.
- b) Waste copies of *PROPRIETARY* information generated in the course of copying, printing, or otherwise handling such information shall be destroyed according to approved procedures (See the Tenet Records Management Policy and Procedure No. 1.11 for further information).

3. Information by Fax

CONFIDENTIAL information may be faxed over unencrypted lines only when time is of the essence and no alternative method with higher-security transmission is available. Faxes sent unencrypted outside of the trusted network should be transmitted in analog form. Faxing *CONFIDENTIAL* information should only be conducted if the following rules are observed, and *PROPRIETARY* information may be faxed under these same guidelines:

- a) If the Fax number has not been previously used, a cover sheet shall first be sent and acknowledged by the recipient. After this test is performed, the *CONFIDENTIAL* and/or *PROPRIETARY* information may be sent.
- b) Unless no other transmission alternative is available and information must be transmitted, *CONFIDENTIAL* and/or *PROPRIETARY* information shall not be faxed via intermediaries (i.e. hotel staff, rented mailbox store staff).


	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 7 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- c) A cover sheet shall be sent as the lead page of the fax. This cover sheet shall include the following information:
- (i) From: Originator's name, company and telephone contact number.
 - (ii) To: The recipient's name, company fax number and telephone number.
 - (iii) The following statement of information confidentiality should be included with all fax transmissions NOT originating in the Law Department: "The information in this communication is confidential and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication."
 - (iv) The following statement of information confidentiality should be included with all fax transmissions originating in the Law Department: "The information in this communication is confidential and may be privileged, and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication."
 - (v) The number of pages in the fax, including the cover sheet.
- d) If the fax is being sent to an internal fax number (4-5 digit number), then the fax cover sheet shall be optional as long as the recipient has some means of determining the fax's originator.

4. Information By E-Mail

E-Mail should only be used to transmit *CONFIDENTIAL* information in accordance with Transmission Procedure No. 8.3.6. E-Mailing *PROPRIETARY* information is permitted when using authorized Tenet e-mail systems, and does not require encryption.

- a) Use of unauthorized mail systems (i.e. Hotmail, AOL Mail, Yahoo Mail), to transmit *CONFIDENTIAL* or *PROPRIETARY* information is prohibited.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 8 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- b) The following statement of information confidentiality should be included with all email transmissions NOT originating in the Law Department: “The information in this communication is confidential and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication.”
- c) The following statement of information confidentiality should be included with all email transmissions originating in the Law Department: “The information in this communication is confidential and may be privileged, and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication.”

5. Instant and Text Messaging

Use of any form of instant messaging (i.e. ICQ, AOL Instant Messenger, MSN Messenger, Yahoo Messenger) to transmit *CONFIDENTIAL* or *PROPRIETARY* information is prohibited.

6. Internal Dissemination of *CONFIDENTIAL* Information

CONFIDENTIAL information may be disseminated internally as follows:


- a) By hand delivery directly to the addressee or a secure area (not left on desks or in unprotected mail slots); or
- b) By internal mail, if it is securely enclosed in an envelope and marked with the appropriate address and as “CONFIDENTIAL” only.

PROPRIETARY information may be sent through internal mail channels. The envelope shall be marked with the appropriate mailing address only.

7. Information on the Phone

CONFIDENTIAL information may be communicated over telephones using the following guidelines:

- a) *CONFIDENTIAL* information shall not be discussed on speakerphones unless all participating parties first acknowledge that unauthorized individuals are not in close proximity.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 9 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- b) Users shall speak in guarded terms and refrain from mentioning *CONFIDENTIAL* details beyond those needed to communicate the information.

8. Public Discussions

Users shall refrain from discussing *CONFIDENTIAL* and *PROPRIETARY* information when holding discussions in public (i.e. hallways, elevators, cafeterias, restrooms). Reasonable safeguards (i.e. lowering voices, changing locations) should be taken to limit inadvertent disclosures of PHI.

9. Information in Meetings


When *CONFIDENTIAL* information is released in a meeting, the speaker shall clearly communicate the sensitivity of the information.

- a) The speaker shall remind the audience to use discretion when disclosing it to others.
- b) Visual aids such as slides and overhead transparencies shall include a *CONFIDENTIAL* label.
- c) Attendance at meetings where *CONFIDENTIAL* information is discussed shall be adequately controlled.

10. Taking Information Off-Site

CONFIDENTIAL Tenet information (which includes, without limitation, portable computers with hard disks, floppy disks, hard-copy output, and paper memos) shall not be removed from Tenet facilities unless such removal is part of the User's required job responsibilities. When taking Tenet information off-site, Users shall ensure that:

- a) *CONFIDENTIAL* information is not left unattended unless it is maintained in a secure location.
- b) Appropriate safeguards are implemented when transporting *CONFIDENTIAL* information, including paper copies of PHI, portable computers storing PHI, and electronic media storing PHI. Vehicles containing *CONFIDENTIAL* information shall be kept locked while unoccupied, and *CONFIDENTIAL* information shall be stored in the trunk when possible.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 10 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

CONFIDENTIAL and *PROPRIETARY* information shall not be read, discussed, or otherwise exposed in public places, such as airplanes, public transportation, or restaurants.

11. Information Storage

CONFIDENTIAL information in hardcopy form or on computer readable media shall be stored in secure fashion when not in use. Options for secure storage include

- a) A locked file cabinet.
- b) A safe.
- c) A secured room.

It is recommended that *CONFIDENTIAL* information on computer media that are stored in secure locations be encrypted using the Data Encryption method outlined in Encryption Control Procedure No. 8.1.3. *CONFIDENTIAL* information on computer media (including backup tapes) that are not stored in secure locations should be encrypted using the Data Encryption method outlined in Encryption Control Procedure No. 8.1.3.


12. Information Disposal

Guidelines for the disposal of Tenet *CONFIDENTIAL OR PROPRIETARY* information are located in the Tenet Records Management Policy and Procedures No. 1.11.


IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following Tenet documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0.
- Information Classification Standard No. 2.1.0.
- User Security Policy No. 3.0.0.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 11 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- Information Access Control Standard No. 3.1.0.
- Access Request and Modification Procedure No. 3.1.1.
- Access Termination Procedure No. 3.1.2.
- Technical, Maintenance and Housekeeping Personnel Supervision Procedure No. 3.1.3.
- User Conduct Standard No. 3.3.0.
- Password Use Procedure No. 3.3.2.
- Physical Safeguards for Information Assets Policy No. 5.0.0.
- Information Asset Secured Area Protection Standard No. 5.1.0.
- Information Asset Open Area Protection Standard No. 5.2.0.
- Security Administration Policy No. 7.0.0.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0.
- UserID Control Procedure No. 8.1.1.
- Encryption Control Procedure No. 8.1.3.
- Information Asset Administration Standard No. 8.2.0.
- Change Control Procedure No. 8.2.1.
- Backup Procedure No. 8.2.3.
- Network Security Administration Standard No. 8.3.0.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.1
	Title: INFORMATION HANDLING PROCEDURE	Page: 12 of 16
		Revised Date: 06/13/06
		Original Date: 10/10/00

- Tenet Administrative Policies and Procedures No. 1.1 “Access to Patient and Medical/Professional Staff Records”.
- Tenet Administrative Policies and Procedures No. 1.9 “Public Release of Information”.
- Tenet Administrative Policies and Procedures No. 1.11 “Records Management”.
- Tenet Human Resources Policies and Procedures No. 032-f “Access to Personnel Records”.
- Tenet Human Resources Policies and Procedures No. 304 “Contacts with Government Regulatory Agencies”.
- Tenet Human Resources Policies and Procedures No. 306 “Records Retention”.
- Tenet Privacy Policies and Procedures No. 1.1.1 “Contracts with Business Associates”.
- Tenet Privacy Policies and Procedures No. 1.3.4 “Patient Right to an Accounting”.

NOTE: This document should be reviewed by regional counsel prior to being distributed to a vendor for signature.

ADDENDUM A

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT ("Agreement"), dated as of the day of _____, 200_, is entered into by _____ ("Party A") and _____ ("Party B").

RECITALS

A. The parties are interested in entering into discussions and negotiations regarding the _____ and entering into a _____ agreement whereby _____. To aid the parties in their determination of whether to enter into such business relationships, access to certain confidential information is necessary.

B. Each party allows the other party to have access to certain confidential information, as described below, in consideration of each party's covenant to keep the information confidential and not use such information for its own use other than as is necessary to determine whether the parties will enter into any business relationship in accordance with the terms hereof.

C. The parties mutually desire to keep the fact of their discussions, communications, and negotiations strictly confidential and to protect such confidential information of one party from use by the other party in any fashion not contemplated by this Agreement.

AGREEMENT

NOW, THEREFORE, in consideration of the foregoing Recitals and of the mutual covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound hereby, the parties hereto mutually agree as follows:

1. **RECITALS.** The recitals hereinabove set forth are true and correct and are incorporated herein.

2. **CONFIDENTIALITY.**

a. In consideration of the discussions, communications, and negotiations contemplated by the parties and of the parties providing each other, or their representatives, with access to certain non-public confidential information about the properties and operations of the other party, each of the parties hereby acknowledges and agrees, for itself and its directors, officers, shareholders, employees, and agents, that all disclosures, explanations, information, documents, writings of whatever nature, in any way related to the other's business, and the entering into of this agreement between Party A and Party B and all proprietary information, patents, copyrights, trademarks, trade names, trade secrets, processes, methods, improvements and licenses associated

Tenet Healthcare Corporation

with the other's business, and all client lists, financial information, information relating to operating procedures, employee information and all other documents and information related in any way to the operation of the other's business or the property of the other party (hereinafter referred to collectively as the "Evaluation Material") are valuable, special, and unique assets of the other party, and are disclosed and given solely to enable each of the parties to evaluate the desirability of entering into a business relationship with the other.

b. Evaluation Material does not include information that (a) is or becomes generally available to the other party or otherwise to the public other than as a result of disclosure to one party by the other party, or (b) is or becomes available to the other party or otherwise to the public on a non-confidential basis prior to its disclosure to one party by the other party, including, without limitation, from a source other than the other party.

3. **EXCLUSIVITY.** During the period of _____ (___) calendar days following Party B's execution of this letter, Party B shall not seek, explore, consider, or entertain offers from any other party relating to his employment or any affiliation or acquisition, in part or in whole, of its _____.

4. **DISCLOSURE.** In order to accomplish the evaluation identified in paragraph 2.a. above, the parties, in reliance upon the covenants contained herein, agree to make certain confidential information available to its representatives. As used herein, the representatives of each party are the directors, officers, shareholders, employees, advisors and agents, including, but not limited to, auditors and bankers, of either party who (i) need to know such information for the purpose of assisting either party in evaluating the desirability of entering into a business relationship with the other party, and (ii) shall have been informed by Party A or Party B, as applicable, of the confidential nature of the Evaluation Material.

5. **RETURN OF INFORMATION.** If, and at such time as, either of the parties has determined not to enter into a business relationship with the other, but in any event no later than three (3) business days from the date of the written demand of either party, each party shall return to the other, during regular business hours by hand delivery or Federal Express or similar courier with guaranteed overnight delivery, all of the Evaluation Material provided by the other, including any copies or representations thereof made by the party.

6. **NON-DISCLOSURE.** The parties each agree, for the benefit of the other, to keep the existence of this Agreement, and the existence, nature, and content of the discussions and investigations made in connection herewith, secret and not to disclose the same to any third party, except as required by a governmental agency or court of competent jurisdiction or as otherwise required by applicable law, without the prior written consent of the other party, which may be withheld in such other party's sole discretion.

7. **CONFIDENTIALITY OF EVALUATION MATERIAL.** The parties each agree, for the benefit of the other, to hold confidential all Evaluation Material made available to the other. Each party agrees that said Evaluation Material shall be used only in the context of the contemplated discussions and negotiations, and as such, it shall not be used for any other purpose or disclosed to any third party outside of either party or either party's representatives, except as required by a governmental agency or court of competent jurisdiction or as otherwise required by applicable law.

8. **REMEDIES.** In the event of a breach or a threat of a breach of this Agreement by either party hereto, or any of its employees, directors, officers, shareholders, partners or agents, the

Tenet Healthcare Corporation

other party shall be entitled to an injunction restraining such party from breach or threat of breach. Nothing herein shall be construed as limiting such party's right to any other remedies available for such breach or threat of breach, including, without limitation, the recovery for damages, including, without limitation, all costs and attorneys' fees for all related proceedings, trials, and appeals and all work required in connection with the enforcement hereof. This covenant shall be deemed to be an agreement independent of any other obligation of the parties hereunder and the existence of any claim or cause of action by one of the parties hereto, whether predicated upon this Agreement or otherwise, or the invalidity of any other provision of this Agreement, shall not constitute a defense to the enforcement of this covenant by the other party hereto.

9. OBLIGATIONS OF THE PARTIES.

a. Unless and until a definitive agreement between Party A and Party B with respect to entering into a business relationship has been executed and delivered, neither Party A nor Party B are under any legal obligation of any kind with respect to such discussions and negotiations by virtue of this Agreement, except for the matters specifically agreed to in this Agreement.

b. The obligations hereunder shall survive the return of the Evaluation Material and shall be binding upon Party A and Party B for a period of six (6) months from the date of return of all of the Evaluation Material.

10. MISCELLANEOUS.

a. This Agreement contains the entire understanding of the parties and shall not be modified except by a writing signed by the parties hereto.

b. No waiver of any right or remedy shall be deemed a waiver of any subsequent right or remedy.

c. This Agreement shall be binding on the successors and assigns of the parties.

d. This Agreement shall be governed by and construed in accordance with the laws of the State of _____.

e. This Agreement may be executed in one or more counterparts, each constituting one and the same original.

f. The parties hereto agree to execute such other documents and writings as may be necessary to effectuate the purposes and intentions set forth herein.

g. In the event either party shall be required to seek legal recourse in order to enforce or effectuate the performance hereof, the materially prevailing party in any litigation shall be entitled to recover all costs and expenses of enforcement, including reasonable attorneys' fees (whether on appeal or otherwise).

THE PARTIES HERETO have executed this Agreement as of the day and year first above written.

Tenet Healthcare Corporation

[NAME OF PARTY A]

By:

Name:

Title:

[NAME OF PARTY B]

By:

Name:

Title: