	<b>Regulatory Compliance Policy</b>	<b>No. COMP-RCC 4.19</b>
	<b>Title:  ELECTRONIC PATIENT RECORD (EPR) POLICY</b>	<b>Page: 1 of 5</b>
		<b>Effective Date: 08-01-08</b>
		<b>Retires Policy Dated: 10-08-03</b>
		<b>Previous Versions Dated:</b>

**I. SCOPE:**

This Policy applies to (1) Tenet Healthcare Corporation and its wholly owned subsidiaries and affiliates (each, an “Affiliate”); (2) any other entity or organization in which Tenet Healthcare Corporation or an Affiliate owns a direct or indirect equity interest of 50% or more; and (3) any hospital or healthcare facility in which Tenet Healthcare Corporation or an Affiliate either manages or controls the day-to-day operations of the facility (each, a “Tenet Facility”) (collectively “Tenet”).

**II. PURPOSE:**

The purposes of this policy are to establish a standardized process for the conversion of the patient medical record from paper to electronic format, to define the legal medical record in this process and to ensure compliance with the requirements contained within the [Corporate Integrity Agreement dated September 27, 2006 between Tenet Healthcare Corporation and the Office of Inspector General of the Department of Health and Human Services](#).

**III. POLICY:**

Each Tenet Facility will create a complete and accurate electronic legal medical record by accepting the images of the paper medical record into the secured electronic document system for archiving and access controls, consistent with all applicable federal and state regulations.

**IV. PROCEDURE:**


A. Tenet Facility Implementation

1. Definition of a Legal Medical Record

The paper medical record is the official legal medical record until after it is available in the secured electronic document system. Once the medical record is available for access via the electronic document system, it then becomes the official legal medical record in electronic format and the paper record is no longer considered the legal record.

2. Electronic Record Accuracy

a. The Health Information Management (“HIM”) Department will ensure the quality of the scanned and indexed documents through continual review of the record as it proceeds through the process of analysis, coding and chart completion. If an error in indexing is identified, or the quality of a scanned image is poor, the error is documented and provided to the designated supervisor.

	<b>Regulatory Compliance Policy</b>	<b>No. COMP-RCC 4.19</b>
	<b>Title:  ELECTRONIC PATIENT RECORD (EPR) POLICY</b>	<b>Page:</b> 2 of 5
		<b>Effective Date:</b> 08-01-08
		<b>Retires Policy Dated:</b> 10-08-03
		<b>Previous Versions Dated:</b>

b. Each page of each document in the electronic patient record will contain a legible patient identifier for the patient treatment episode that the record represents. The chart prep clerk verifies the account number on each document. The chart scanning clerk monitors the scanner hopper to assure there are no misfeeds. The Indexing clerk verifies the quality of the image. Either the scanning or indexing clerk must verify that each side of each document has been scanned and that a quality image is captured. Additional ongoing checks take place at the time of analysis and coding.

c. Errors identified through the various checks for accuracy of the record are tracked by personnel.

d. To ensure the continual monitoring for quality of the electronic patient medical record, the HIM department will review each month, a minimum of five (5) records scanned/indexed by each clerk to ensure that each document is scanned and indexed to the established standards. That is, a comparison of each page in a paper record against the scanned images. Findings of these reviews will be shared with the clerk to provide a means for education, correction, and feedback.


### 3. Privacy of the Electronic Medical Record

#### a. Privacy of the Database

- (1) Only authorized personnel have direct access to the databases and/or images of the electronic patient record file system utilized by the Tenet Facility.
- (2) Personnel given access to the system must demonstrate competence in using computer technology and database query language.
- (3) The database passwords are limited to those staff members who are experienced with database query language and database management. The staff members are considered to be System Administrators and this access is limited.

#### b. Privacy of the Electronic Patient Record

- (1) User access to the documents is done by database entries based upon the user commands in the application.

	<b>Regulatory Compliance Policy</b>	<b>No. COMP-RCC 4.19</b>
	<b>Title:  ELECTRONIC PATIENT RECORD (EPR) POLICY</b>	<b>Page:</b> 3 of 5
		<b>Effective Date:</b> 08-01-08
		<b>Retires Policy Dated:</b> 10-08-03
		<b>Previous Versions Dated:</b>

- (2) HIM department staff have access to Adjust Document Indexes in the application, which allows them to re-index documents, i.e. change the document type. They also have access to delete documents. This type of access is audited through the audit trail.
- (3) All users of the system, including physicians, must sign the Security Request Form (as approved by the HPF Users Group – Attachment A).
- (4) Backups to safeguard the data are performed as described in the IS Department Policies and Procedures for back up of electronic patient record files.
- (5) The servers are located in secure areas, requiring pass codes to enter the area.


#### 4. Auditing

a. The system maintains an audit trail that provides a record of user, action and date of action for the system and medical record access. Reports are available from the EPR depending on the user's security rights.

b. Reports are used to research any allegations of inappropriate access of records and when an event occurs, the issue is handled through the human resources and/or medical staff disciplinary actions.

c. The reports include the account number, patient name, medical record number, name of person taking the action, the action taken and the date the action occurred. This includes reporting the processing performed by the software agents of the system.

d. User access audits, using the Corporate Audit Reports stored on the HPF Monitor web page, shall be completed at least monthly. These audits shall include a review of selected physician and Tenet Facility staff members who have access to EPRs. The audit shall include a review of records accessed by selected users to determine if information accessed was limited to a "need to know" basis. Where it is discovered that a user accessed a record he/she did not need to access to perform their job responsibilities, corrective action (mitigation and sanctions) shall be taken.

	<b>Regulatory Compliance Policy</b>	<b>No.</b>	<b>COMP-RCC 4.19</b>
	<b>Title:</b>	<b>Page:</b>	<b>4 of 5</b>
	<b>ELECTRONIC PATIENT RECORD (EPR) POLICY</b>	<b>Effective Date:</b>	<b>08-01-08</b>
		<b>Retires Policy Dated:</b>	<b>10-08-03</b>
		<b>Previous Versions Dated:</b>	

e. Additional random audits shall be completed when a patient is admitted who is considered a “VIP” patient (movie star, member of the Tenet Facility workforce, athlete, etc.). The access to the record for this VIP patient shall be reviewed monthly. Where it is discovered that a user accessed a record he/she did not need to access to perform their job responsibilities, corrective action (mitigation and sanctions) shall be taken.

#### 5. Paper Document Retention

a. After the paper medical record has been accepted into electronic format, the paper patient medical record will be boxed and stored. A business associate agreement will be executed with all off-site storage vendors.

b. The HIM Director will maintain a Master List of boxes, by date, including a list of the content of each box, sent for storage.

c. The retrieval of any stored boxes requires the approval of the HIM Director.

d. The paper documents will be stored for six (6) months after the discharge date and destroyed consistent with [Administrative Policy AD 1.11, Records Management](#).

#### B. Enforcement


All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy will be subject to appropriate disciplinary action pursuant to all applicable policies and procedures, up to and including termination. Such disciplinary action may also include modification of compensation, including any merit or discretionary compensation awards.

#### V. REFERENCES:

- [Corporate Integrity Agreement dated September 27, 2006 between Tenet Healthcare Corporation and the Office of Inspector General of the Department of Health and Human Services](#)

- [Administrative Policy AD 1.11, Records Management](#)

- [Patient Privacy Policy and Procedure 1.2.2 Minimum Necessary Procedure](#)

	<b>Regulatory Compliance Policy</b>	<b>No.</b> COMP-RCC 4.19
	<b>Title:</b>	<b>Page:</b> 5 of 5
	<b>ELECTRONIC PATIENT RECORD (EPR) POLICY</b>	<b>Effective Date:</b> 08-01-08
		<b>Retires Policy Dated:</b> 10-08-03
		<b>Previous Versions Dated:</b>

- [Patient Privacy Policy and Procedure 1.2.3 Use and Disclosure Procedure](#)
- [Information Security Policies and Procedures COMP-Sec 3.0.0 User Security Policy](#)
- [Information Security Policies and Procedures COMP-Sec 3.3.0 User Conduct Standard](#)

**VI. ATTACHMENTS:**

- Attachment A - HPF System Security Request Form



**HPF SYSTEM SECURITY REQUEST FORM**

<b>ADD NEW USER ID</b>	<b>ADD FUNCTION TO EXISTING ID</b>	<b>REMOVE FUNCTI ON FROM ID</b>	<b>CHANGE FUNCTION ON EXISTING ID</b>	<b>DISABLE USER ID  ID TO BE DELETED (REQUIRED)</b>	<b>TERMINATED EMPLOYEE</b>
------------------------------------	--	---	---	---	--------------------------------

<b>SECTION A</b>	<b>REQUESTOR INFORMATION – TO BE COMPLETED BY REQUESTOR – REQUIRED</b>
------------------	--

FIRST NAME	MIDDLE INITIAL	LAST NAME	WORK: AREA CODE/ NUMBER/ EXT.
JOB TITLE/DEPARTMENT		EMAIL ADDRESS	LAST FOUR DIGITS OF SOCIAL SECURITY #
FACILITY NAME		eTENET USER ID	FACILITY NUMBER(S)

USER TYPE:

FACILITY <input style="width: 20px; height: 20px;" type="checkbox"/>	CORPORATE <input style="width: 20px; height: 20px;" type="checkbox"/>	REGIONAL <input style="width: 20px; height: 20px;" type="checkbox"/>	MARKET <input style="width: 20px; height: 20px;" type="checkbox"/>	OTHER <input style="width: 20px; height: 20px;" type="checkbox"/>	PLEASE SPECIFY _____
--	---	--	--	---	-------------------------

---

## Security Statement

Computer access privileges are granted to Tenet employees at the lowest possible level pursuant to the efficient performance of the employee's duties and must be used only for Tenet authorized business. Computer access devices, such as user identity codes and passwords, remain the property of Tenet and are not to be divulged to any other person unless approved by Perot Systems Security. Unauthorized access to, use and possession of, removal of, and/or damage to company records is a breach of the Tenet corporate policy and may result in disciplinary and/or legal action.

I have read and understood the content of the above Security Statement and agree to accept and abide by the policies stated herein.

I agree to keep my access code confidential and to guard the confidentiality of all system information. As a Tenet employee, I share responsibility for the protection of Tenet's information assets and will be held accountable for maintaining their integrity, confidentiality, and availability.

Access to data outside of your home (authorized) facility or region is limited due to Federal (JCAHO), Corporate, and Internal Audit guidelines protecting patient confidentiality and data security. Additional authority will be required for these requests.

Violation of this policy will be grounds for disciplinary action, up to and including termination. Tenet Healthcare Corporation reserves the right to pursue legal prosecution under local, state, and federal statutes.

### **This Subsection on Electronic Signature Notification is Applicable to Physicians Only**

TO: \_\_\_\_\_

Chief Executive Officer

This is to inform you of my intent to electronically authenticate transcribed interpretations of dictated reports, as well as any entries, written orders, or instructions through the use of a unique, confidential PIN number assigned specifically to me.

I am the only person to whom this code is assigned. I am responsible for all entries that I record into the computer system. I will neither delegate my assigned code to any other person, nor allow any other person to use it for authentication of such transcribed reports or entries.

**USER/PHYSICIAN  
SIGNATURE (REQUIRED)** \_\_\_\_\_

DATE \_\_\_\_\_

**SECTION A****AUTHORIZATION SIGNATURE – REQUIRED**

SUPERVISOR NAME \_\_\_\_\_ DATE \_\_\_\_\_

SUPERVISOR SIGNATURE \_\_\_\_\_ PHONE \_\_\_\_\_

HIM DIRECTOR/SECURITY ADMINISTRATOR NAME \_\_\_\_\_ DATE \_\_\_\_\_

HIM DIRECTOR/SECURITY ADMINISTRATOR SIGNATURE \_\_\_\_\_ PHONE \_\_\_\_\_

CORPORATE SPONSOR SIGNATURE (IF APPLICABLE) \_\_\_\_\_ PHONE \_\_\_\_\_

HOSPITAL SPONSOR SIGNATURE (IF APPLICABLE) \_\_\_\_\_ PHONE \_\_\_\_\_