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 greater than 50%; 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 "Hospital") (collectively, "Tenet").

II. PURPOSE:

The purposes of this policy are to establish parameters for the contents and maintenance of patient medical records and to define the components that constitute the legal medical record for Hospital.

III. DEFINITIONS:

A. "**Administrative Data**" means patient identifiable information used for administrative, regulatory and healthcare operations and financial purposes. Examples of administrative data include authorizations for release of information, correspondences, birth and death certificates, coding abstracts or summaries, quality and utilization reporting and administrative reports.

B. "**Legal Medical Record**" means the collection of information created and maintained in the ordinary course of Hospital's business, in accordance with this policy, made by a person who has knowledge of the acts, events, opinions or diagnoses related to the patient, and made at or around the time indicated in the documentation as further defined in this policy. The Legal Medical Record does not include health records that are not created and maintained by or on behalf of Hospital, such as patient health records created by other facilities, except to the extent that such records are integrated into Hospital's patient record to fulfill record content requirements, such as a history and physical prepared in a physician office and submitted as a part of the required history and physical for an inpatient

C. "**Designated Record Set**" means the group of records that includes protected health information and is maintained, collected, used or disseminated by, or for, Hospital for each individual who received care from Hospital and its medical staff. The Designated Record Set includes Hospital's medical record and billing records and any other information used, in whole or in part, to make decisions about individuals.

D. "**Medical Record**" means the compilation of information contemporaneously created for every patient who receives services at Hospital.

E. "**Research Records**" means those records which are created specifically for the purpose of conformance with the terms of a research protocol or clinical trial and which would not be created absent the patient's participation in the applicable trial. Research records do not include clinical documentation regularly created for

patients who receive the same service outside of a research trial. Research records are not part of the legal medical record.

F. "**Secondary Patient Information**" means summaries of material contained in the legal medical record, source data from outside of the legal medical record, administrative data, derived data, drafts, audio and video recordings of patient encounters, works in progress, and audit trails. Additionally, clinical decision-making tools, such as alerts and pop-ups are not part of the legal medical record. Secondary patient information is not part of the legal medical record, except that such records may be designated as a part of the legal medical record when necessary for the evaluation and subsequent treatment of the patient at Hospital.

G. "**Source Data**" means data generated by clinical systems to the extent captured in the designated electronic records database. Examples may include portions of cardiac monitoring or fetal monitoring strips that have been transmitted to the record database.

IV. POLICY:

The Hospital will create a complete and accurate legal medical record through a secure electronic database which includes, as applicable, electronic data created by Hospital's electronic medical record system and images of paper medical records, as well as designated source data in the absence of documentation or interpretations.

V. PROCEDURE:

A. Hospital will create a medical record for every patient. It is acknowledged that Hospital is implementing various electronic health record systems. Thus, each element of the medical record will be created and maintained in paper or electronic form, as Hospital deems appropriate from time to time during the patient's encounter at Hospital.

B. The legal medical record is comprised of those elements identified on Attachment A to this policy, to the extent that any of these elements may apply to a particular patient, each of which shall be in paper or electronic form as may be designated by Hospital from time to time, until the patient has been discharged and the entire legal medical record is available in the secure electronic record databases. Thereafter, the paper elements which have been scanned shall no longer be deemed a part of the legal medical record.

C. Preliminary reports and documents are available for patient care as a part of the medical record until they are authenticated. They are not part of the legal medical record. Once authenticated, the final report will become part of the legal medical record.

D. Secure Electronic Record Databases

1. The legal medical record will be stored in one or more secure electronic record databases, which will be accessible only to authorized individuals consistent with their role in the care of the patient or the operations of Hospital.

2. Upon a patient's discharge from Hospital, the Health Information Management (HIM) Department will ensure that paper components of the legal medical record are timely retrieved from each clinical unit and scanned and indexed into the secure electronic record databases.

   a. HIM 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. Each page of each document in the secure electronic record databases 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. Elements of the legal medical record which are not initially created or maintained in paper form will be entered into the secure electronic record databases as deemed appropriate by Hospital from time to time. Options to perform this function include electronic data feeds, printing of the material from the initial source system and scanning it into the secure electronic record database in the same manner as paper records and such other alternatives as Hospital may determine will provide a complete and accurate legal medical record.

   d. To ensure the continual monitoring for the quality of electronic patient records, the HIM department will review each month a minimum of five records scanned/indexed by each clerk to ensure that each document is scanned or otherwise entered into the secure electronic record databases according to established standards. Findings of these reviews will be shared with the clerk as a means for education, correction and feedback.

e. Additionally, the Hospital may adopt automated systems to electronically monitor the interfaces and processes by which data from clinical and electronic health record systems populate the secure electronic record databases to ensure that this data reaches the secure electronic record databases as intended

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

3. Privacy

a. Access to the secure electronic record databases will be password protected.

b. Personnel will be granted access to the secure electronic record databases in accordance with standards for appropriate users, competence in computer technology and database query language.

c. User access to documents is based on the user commands in the application.

(1) The HIM Department staff will have access to adjust document indexes in the application, which allows them to reindex documents, i.e, to change the document type. They also have access to delete documents. This type of access is audited through the audit trail.

(2) All users with access to the secure electronic record databases, including physicians, must obtain access via Tenet's approved processes.

(3) Backups to safeguard the data are performed as described in the IS Department Policies and Procedures for back up of electronic records, including the legal medical record.

(4) The servers on which the secure electronic record databases are stored are located in secure areas, requiring passcodes to enter the area.

d. Except as otherwise permitted by this policy or required by law, original paper records may not be removed from the Hospital.

4. Monitoring

a. The system maintains an audit trail that provides a record of user, action and date of action for the system and medical records access.

Reports are available from the secure electronic record databases 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 processes. Allegations of inappropriate access shall be referred to the Compliance Officer/Privacy Officer ("CO") for investigation.

c. Hospital's HIM Director or designee shall monitor user access, according to the monitoring program described in Attachment B. This monitoring will include all persons who have access to the secure electronic record databases. The monitoring shall include a review of records accessed by selected users to determine if information accessed was limited appropriately based on the role and legitimate Hospital purposes of the person accessing the record. Where it is discovered that a user accessed a record in a manner not required by the user's legitimate job functions, the HIM Director will contact the CO.

d. Hospital's HIM Director or designee will complete additional monitoring when a patient is admitted who is considered a "VIP" patient (*e.g.*, movie star, member of the Hospital workforce, athlete). The access to the record of the VIP patient will be reviewed not less often than monthly and for a period not less than 30 days following discharge. Where it is discovered that a user accessed a record in a manner not required by the user's legitimate job functions the HIM Director will contact the CO.

5. Paper Document Retention

a. After the paper medical record has been accepted into the secure electronic record database, the paper patient clinical record will be boxed and stored.

b. The HIM Director will maintain a master list of boxes by date, including a list of the contents of each box.

c. The retrieval of stored documents requires approval of the HIM Director.

d. All paper documents will be stored for a minimum of thirty days after the paper medical record has been accepted into the secure electronic record database and thereafter would be eligible for destruction consistent with Administrative policy AD 1.11, Records Management and its Record Retention Schedule.

6. Release of Records.

The Hospital will release the legal medical record as appropriate under Tenet's Information Privacy and Security Program policies.

E. Responsible Person

The Hospital HIM Director is responsible for assuring that all personal adhere to the requirements of this policy, that these procedures are implemented and followed at the Hospital, and that instances of noncompliance with this policy are reported to the CO.

F. Auditing

The Regional HIM Directors shall audit adherence to this policy, including completion of the user access monitoring program. Audit Services shall audit compliance to this policy as part of its full scope audits.

G. 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 performance management pursuant to all applicable policies and procedures, up to and including termination. Such performance management may also include modification of compensation, including any merit or discretionary compensation awards, as allowed by applicable law.

VI. ATTACHMENTS:

- Attachment A: Elements of Legal Medical Record

- Attachment B: User Access Monitoring Program

Elements of Legal Medical Record

	Cerner	HPF	Paper
Administrative Information			
Registration Form			
Conditions of Service			
Notice of Privacy Practices Acknowledgement			
Advance Directive Acknowledgement			
Advance Directives			
Surrogate Decisionmaker Designations			
Consent Forms			
Patient Belongings Inventory			
AMA Form			
Advanced Beneficiary Notice			
Important Message from Medicare			
Patient Choice Form			
Medical Necessity Form			
Preadmission			
Ambulance Report/EMS Transfer of Care			
Interfacility Transfer Form			
Emergency Department			
Emergency Department Registration form			
Triage Documentation			
ED Physician Notes			
ED Nursing Documentation			
Trauma Record			
Physician Documentation			
History and Physical			
Procedure Note/Operative Report			
Progress Notes			
Orders			
Consultation Reports			
Discharge Summary			
Anesthesia Record			
Query Form/Response			
Nursing Documentation			
Nursing Admission Assessment			
Nursing Assessments			
Nursing Notes			
Graphic Records			
Diabetic Record			
Ancillary Services			
Case Management/Social Services Notes			
Dialysis Records			
Respiratory Care			
Physical Therapy			
Occupational Therapy			
Speech Therapy			
Nutrition Services			

	Cerner	HPF	Paper
Wound Care Notes			
Laboratory			
Hospital Laboratory Reports			
External Laboratory Reports			
Pharmacy			
Medication Administration Records			
Medication Reconciliation			
Sliding Scale			
Pathology			
Pathology Reports			
Radiology			
Radiology Reports			
Other Diagnostics			
Interpretive Reports			
EEG (selected)			
Rhythm Strips (selected)			
Obstetrics/Newborn			
Prenatal History Forms			
Labor Record			
Delivery Record			
OB Assessment			
Newborn Assessment			
Newborn Hearing Test			
Newborn Phototherapy			
Fetal Monitoring Strips			
Birth Certificate Information			
Patient Education			
Discharge Instructions			
Emergency Department Summary Record			
Psychiatry			
Therapy Notes			
Miscellaneous			
Autopsy Reports			
Immunization Records			
Implant Record			
Restraint Documentation			
Resuscitation Records			
Organ Donor Information			
Death Summary			
Photographs (clinical)			
Blood Transfusion			
Referrals for Support Services			
Physics Documents (Radiation Oncology)			
Short Stay Record			
Disposition at Discharge			

Notwithstanding the designation of the electronic clinical record, HPF or paper as the repository of an element of the legal medical record, it is recognized that circumstances, such as computer system downtown, may require a document ordinarily created in electronic form to be created in alternative form and to be maintained as a part of another component of the record system. The documents which are defined to be part of the legal medical record shall be part of such record even if maintained in a secure location other than the record system designated above.

User Access Monitoring Program

Hospital HIM Directors shall review the following reports on a monthly schedule to audit/monitor user activity:

1. Users who Access MRNs of Patients with the Same Last Name

   This report can help identify users who may have accessed their own medical records inappropriately or the medical records of family members without proper authorization.

2. MRNs Printed per User

   A user who has printed far more MRNs during the period than his/her peers may indicate a user who is not following the correct processes that could lead to the inappropriate use or disclosure of PHI.