	Administrative Policy	No.	AD-1.11
	Title: RECORDS MANAGEMENT	Page:	1 of 4
		Effective Date:	09-27-11
		Retires Policy Dated:	03-01-11
		Previous Versions Dated:	01-31-08 08-01-01; 10-01-96

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 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 “Tenet Facility”) (collectively, “Tenet”).


II. PURPOSE:

This Records Management policy is designed to promote a wide variety of goals and objectives, including:

- A. compliance with all applicable laws and regulations mandating retention of certain types of records;
- B. preservation of all records that may be relevant to any ongoing or expected litigation, audits, or government investigations;
- C. enhancement of organizational efficiency by ensuring that information of business value is preserved and readily accessible for appropriate periods of time;
- D. reduction of operational costs by expediting the process of locating needed records and eliminating the retention and storage of unneeded records;
- E. ensuring that records of no continuing value are periodically superseded or destroyed, and that all records destruction occurs in compliance with approved policies and procedures;
- F. safeguarding essential information of critical significance; and
- G. ensuring that records containing confidential or proprietary information will be securely maintained, controlled, and protected to prevent unauthorized access.

III. DEFINITIONS:

- A. **“Record”** means, for purposes of this policy, any recorded information, regardless of format or media. This includes, but is not limited to, documents, medical records, papers, letters, books, pamphlets, maps, photographs, microfilm, x-rays, drawings, charts, cards, audio or video recordings, magnetic tapes, e-mail, electronic images, and information contained on computer disks, databases, or electronic file systems, whether duplicates or originals, that are generated and/or received.


	Administrative Policy	No.	AD-1.11	
	RECORDS MANAGEMENT	Title:	Page:	2 of 4
		Effective Date:	09-27-11	
		Retires Policy Dated:	03-01-11	
		Previous Versions Dated:	01-31-08 08-01-01; 10-01-96	

- B. “**Contractor**” means any authorized entity or individual engaged through contract or otherwise to perform services on behalf of Tenet.
- C. “**Records Retention Schedule**” means the document identifying certain types of records that, for business and/or legal reasons, are subject to mandatory retention for a specified period of time.
- D. “**General Retention Rule**” means the general principle that all records not specifically identified by the Records Retention Schedule may be discarded at any time but may not be retained for longer than one year following the date upon which they were created or received. Drafts and informational copies of records are subject to this General Retention Rule unless the Records Retention Schedule specifically provides otherwise. Instant Messages and Voicemail are most commonly used for transitory communication and are covered by the General Retention Rule.
- E. “**Legal Hold Notice**” means a legal notice requiring retention of certain records that may be relevant to matters that are subject to litigation, government investigations, or audits.

IV. POLICY:

All records shall be maintained in compliance with the Records Retention Schedule or, if applicable, the General Retention Rule defined in this policy. The current version of the Records Retention Schedule can be accessed through eTenet on the [Records Management SharePoint site](#). From time to time, the Law Department may issue a Legal Hold Notice requiring suspension of document destruction relating to specific records. Compliance with all Legal Hold Notices is mandatory. This policy applies to all records created, received, or maintained in the course of Tenet’s business, regardless of the content of such records or their location.

- A. Records created or stored in an employee’s “personal” working files, at an employee’s home, or on personally owned computers or personal digital assistants (PDAs) are also subject to this policy if such records were created or received in the course of Tenet business.
- B. Any record generated or received utilizing a Tenet system or resource (including computers, email, fax machines, phones, or software) is considered a Tenet business record and hence is subject to this policy, if such records were created or received in the course of Tenet business.
- C. This policy also extends to records created for Tenet’s use or benefit by third-party contractors or authorized agents.

	Administrative Policy	No.	AD-1.11
	Title: RECORDS MANAGEMENT	Page:	3 of 4
		Effective Date:	09-27-11
		Retires Policy Dated:	03-01-11
		Previous Versions Dated:	01-31-08 08-01-01; 10-01-96

V. PROCEDURE:

A. Legally Required Suspension of Policy

This policy may be suspended in whole or in part at any time if circumstances arise - such as litigation, government investigations, or audits - which legally require the retention of records that might otherwise be subject to disposal. In the event that suspension of the policy is required, the Law Department will issue a Legal Hold Notice notifying relevant employees concerning the nature and scope of the suspension. Legal Hold Notices remains in effect until withdrawn by the Law Department. Destruction of records in violation of Law Department instructions could result in prosecution for obstruction of justice or contempt of court. Any employee who becomes aware of actual or potential litigation or other circumstances that could warrant suspension of this policy should promptly notify the Law Department.

B. Oversight and Implementation

The Tenet Records Management Committee will oversee implementation of this policy and will coordinate regular efforts to ensure compliance. In addition, each Tenet Facility, as well as each corporate office, shall designate one or more “Records Coordinators” to be responsible for implementing and maintaining Tenet’s records management program at their location. Questions about the policy should be directed to the designated Records Coordinator.

C. Storage and Destruction of Records


For all Tenet active and divested facilities, procedures for storing and destroying records are available on the [Records Management SharePoint site](#).

D. Instant Messages and Voice Mail

Employees should not use Instant Messages or Voicemail to create Records that have a specific retention period on the Records Retention Schedule. For administrative purposes, Tenet may choose to retain Instant Messages, Voicemail, or other forms of transitory communication for a temporary period of time not to exceed one year.

E. Retention Schedule Questions

Although Tenet is dedicated to maintaining a Records Retention Schedule that is at all times comprehensive, accurate, and current, there could be instances in which the Records Retention Schedule omits an important category of records or specifies a retention period that is too short. In either case, a literal reading of the Records Retention Schedule may result in premature destruction of records. If at any time an

	Administrative Policy	No.	AD-1.11
	Title: RECORDS MANAGEMENT	Page:	4 of 4
		Effective Date:	09-27-11
		Retires Policy Dated:	03-01-11
		Previous Versions Dated:	01-31-08 08-01-01; 10-01-96

employee believes that the Records Retention Schedule may be incomplete or inaccurate, the employee should contact the Facility's Records Management Coordinator or Hospital Compliance Officer (HCO) before taking further action. Records Coordinators may request a review, addition or deletion to the Records Retention Schedule. A form to be used in this process is available on the [Records Management SharePoint site](#) on eTenet.

F. Legal Penalties for Improper Document Alteration, Destruction, or Concealment

Federal law provides that anyone who knowingly destroys, mutilates, conceals, or falsifies any record or tangible object with intent to impede, obstruct, or influence proceedings involving federal agencies or bankruptcy proceedings, or who otherwise attempts to alter records or other objects with the intent to impair the integrity or availability of the record or object to an official proceeding, may be fined and/or imprisoned. Employees with questions about the legal propriety of destroying certain records should contact the Law Department before taking any action. Information pertaining to unauthorized destruction, removal, or use of Tenet records or regarding falsification or inappropriate alteration of information in a record should be immediately reported to the HCO assigned to the Facility.

G. Conifer Provision

Notwithstanding anything to the contrary contained in this policy, this policy shall not apply to Conifer Health Solutions, Inc. and its subsidiaries (collectively, "Conifer") with respect to Records that Conifer receives, possesses, or creates for Conifer's non-Tenet clients ("Third Party Records"). Third Party Records will be subject to the Conifer Records Management policy for Third Party Records. For purposes of clarification, all Conifer Records that do not constitute Third Party Records will be governed by this policy.

H. Auditing and Monitoring

Tenet's Audit Services Department shall audit adherence to this policy in its routine audits.

I. 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.



POLICY FLASH

Date: September 29, 2011

To: Distribution List

From: Sarah E. Campbell, Director, Policies and Procedures Management
Jim Roche, Director, Records Management

Subject: Updates to Records Management Policy

On September 26, 2011, Tenet's Corporate Integrity Agreement (CIA) with the Office of the Inspector General of the Department of Health and Human Services expired. The CIA included a document and record retention requirement that was incorporated into Tenet's [Administrative policy AD 1.11 Records Management](#) and corresponding Record Retention Schedule. As a result of the CIA's expiration, we have revised the policy to reflect that we are no longer under a CIA. To access the revised policy and retention schedule on the Monitor page of eTenet, [click here](#) (*eTenet login required*).

Although the CIA has expired, our record retention obligations continue. The purpose of this memo is to explain how to handle records that were subject to the CIA retention requirements.

The CIA required Tenet to maintain records for a minimum of 6 years unless the records were subject by law to a longer retention period. To address this requirement, our schedule included an Assigned Retention Period identified as **CIA**. Records given this Assigned Retention Period do not have another, longer retention period required by law and must be kept a minimum of 6 years once they are no longer active. We also added two categories, **Ethics Compliance: Corporate Integrity Agreement Compliance** (COM1050) and **Compliance: Corporate Integrity Agreement Compliance** (COM6010) for records that did not fit other categories.

We have updated the name of the Assigned Retention Period from **CIA** to **COM** (for compliance). The time period will remain the same, a minimum of six years after the records are no longer active or required by law. As with all other types of records, if the records also fall into a record category with a longer retention period, the longer time period governs.

We also have updated both category names from **Corporate Integrity Agreement Compliance** to **General Compliance**. We updated the definition so that it includes all records documenting compliance activities not otherwise specified in another category. Any record classified as COM1050 or COM6010 during the CIA remains in these categories today.

[Click here](#) to access the policy redline through eTenet's [Policy Central](#) (*eTenet login required*).

We appreciate your review of this Policy Flash and the revised Records Management policy. Please contact Jim Roche should you have any questions. His telephone number is 469.893.6082 and his email address is james.roche@tenethealth.com.