	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>	<b>Page: 1 of 9</b>
	<b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

## I. PURPOSE:

The purpose of this standard is to provide direction for Tenet regarding auditing and monitoring requirements. Logging and auditing of actions within networks, systems, and applications supports the security risk management initiatives for information assets owned by Tenet.

## II. DEFINITIONS:


- A. “**Administrators**” mean the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.
- B. “**Activity Log**,” “**Audit Log**” or “**Audit Trail**” is a series of records of computer events, about an operating system, an application, or user activities. A computer system may have several audit logs, each devoted to a particular type of activity.
- C. A “**User**” means an individual that inputs/outputs data to/from Tenet information assets. These individuals are collectively referred to as Users, and may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, business partners and electronic (web site) visitors.
- D. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.

## III. STANDARD:

Tenet Information Systems will provide sufficient audit log data to support incident investigation, user monitoring and comprehensive audits of compliance with the Information Privacy and Security Program. Tenet reviewers will review certain audit log activities that occur on networks, systems, and applications to monitor potential risks. This standard includes, but is not limited to, systems that store Patient Health Information (PHI), Personally Identifiable Information (PII) and/or Payment Card Industry (PCI) cardholder data.

### A. Recording Audit Logs/Trails:

An audit log/trail must include sufficient information to establish what events occurred and who (or what) caused them. Where available, an event record must specify when the event occurred, the uniquely identifiable attributes (*e.g.*, Host Name, UserID, IP Address, MAC Address) associated with the event, the program or command used to initiate the event, and the result. External-facing systems or technologies must write audit logs to a secure, centralized, internal log server or media device in real-time.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page:</b> 2 of 9
		<b>Effective Date:</b> 08-31-17
		<b>Retires Policy Dated:</b> 10-27-16
		<b>Previous Versions Dated:</b> 09-16-13; 12-22-04; 11-06-00


B. In addition, these identified audit trails must be maintained for PCI-DSS Compliance for at least one year; at least three months of history must be immediately available for analysis

- All individual access to identified in-scope networks, components, or systems.
- All actions taken by any individual with root or elevated administrative privileges.
- Any access to all maintained audit trails.
- Invalid logical access attempts.
- Use of and changes to identification and authentication mechanisms including all elevation of privileges, and all changes, additions, or deletions to accounts with root or administrative privileges.
- Initialization, stopping, or pausing of the audit logs.
- Creation and deletion of system-level objects.

1. Security Event Logging Detail

Logs must be created that can be used to monitor activities that can affect network, system or application security. These logs must record the following:

- a. Intrusion activity
  - (1) Failed login attempts
  - (2) Failed password change attempts
- b. UserID administration activity
  - (1) Modifications
  - (2) Additions
  - (3) Deletions
  - (4) Disabling
  - (5) Changes to the privileges of users
- c. System activity
  - (1) Start-up
  - (2) Shut-down

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page:</b> 3 of 9
		<b>Effective Date:</b> 08-31-17
		<b>Retires Policy Dated:</b> 10-27-16
		<b>Previous Versions Dated:</b> 09-16-13; 12-22-04; 11-06-00

- d. Hardware
  - (1) Hardware and disk media errors
  - (2) Maintenance activity
- e. System anomalies
  - (1) Initialization sequences
  - (2) Logons and errors
  - (3) System processes and performance
  - (4) System resources utilization


## 2. Critical Security Device Protection Logging Detail

Logs must be created that can be used to monitor activities on perimeter devices, including firewalls, routers, switches and other security devices. These logs must record the following:


- a. Device activity
  - (1) Packet screening denials originating from trusted and un-trusted networks
  - (2) User account management
  - (3) Modification to security configuration changes (e.g., Access Control Lists, Firewall rules, Intrusion Protection rules)
  - (4) Application errors (e.g., Web Application errors, Web Services)
  - (5) System errors (e.g., Kernel failure, Kerberos)
  - (6) System shutdown and reboot

## 3. User Activity Logging Detail

Logs must be created in such a manner that individual events are attributed to individual UserIDs. Applications must log activity using the following guidelines:

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 4 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>


- a. User activity must be logged at the field level, and must record the following:
  - (1) UserIDs
  - (2) Access date/time
  - (3) User Access
  - (4) Success or failure indication
  - (5) Origination of event
  - (6) Record access
  - (5) Field access
  - (6) User Actions
  - (7) Additions at the record and field level
  - (8) Modifications at the record and field level
  - (9) Deletions at the record and field level
- b. If user activity cannot be logged at the field level, activity logging must be maintained at the record level, and must record the following:
  - (1) UserIDs
  - (2) Action date/time
  - (3) User Access
  - (4) Success or failure indication
  - (5) Origination of event
  - (6) Identity of affected record
  - (7) Record access
  - (8) User Actions
  - (9) Additions at the record level

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 5 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- (10) Modifications at the record level
- (11) Deletions at the record level
- c. If user activity cannot be logged at the record level, activity logging must be maintained at the system access level and this decision must be documented in the Information Privacy and Security Control Exceptions Book. User activity at the system access level must be recorded, including:
  - (1) UserIDs
  - (2) Logon date/time
  - (3) Logoff date/time
  - (4) Password change date/time
  - (5) Applications invoked
  - (6) Success or failure indication
  - (7) Origination of event
  - (8) Identity of affected data, system component, or resource
  - (9) Attempted access to unauthorized data
  - (10) Use of authorized advanced privileges (security bypass, etc.)
  - (11) Changes to critical application system files
  - (12) Other auditable events, where available
- 4. Backup, Archive, and Protection
 

Log files must be saved to tape or other media and secured in off-site or other appropriate storage. Log files must be backed up according to this procedure and EC.PS.04.05 Technical Controls Security Standard.

  - a. Roll logs (activate a new log, save the old log) rather than overwrite them (use the same log again, losing data).
  - b. Log files are Confidential and must be protected such that no individual can modify or delete the logs.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 6 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- c. Write logs for external-facing systems or technologies to a secure, centralized, internal log server or media device.
- d. Individuals authorized to view logs include members of the compliance staff, the internal audit staff, systems security staff, or systems management staff.
- e. If an unauthorized individual needs access to these logs, they must request access in writing and obtain written permission from the Tenet Facility Information Security Officer.

5. Backup Retention

Log files must be retained for a period of time in accordance with Administrative policy AD 1.11 Records Management and its Record Retention Schedule.

6. Clock Synchronization

The internal clocks of systems that generate activity on Tenet networks and applications must reflect the current time accurately. Date and time can help determine if the user was a masquerader or the actual person specified.

- a. The Home Office Information Systems Department must provide the functionality for clock synchronization.


7. Deactivation, Modification, or Deletion

Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

B. Monitoring User Accounts and Activity


A user Audit Log/Trail logs user activity in a system or application by recording events initiated by the user (*e.g.*, access of a file, record or field).

1. The designated Tenet Facility reviewer(s) for each information system must have knowledge of the workforce members' roles and responsibilities in the organization.
2. All activity monitoring reports must be maintained in Compliance Matters.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 7 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

3. Unless required by law, monitoring reports for clinical systems must not be combined with a patient's clinical record and must not be disclosed beyond authorized use.
4. Examples of Monitoring Reports:
  - a. High Risk Report: Tenet must identify high risk areas to monitor. This report identifies certain high risk scenarios, such as monitoring employee access to VIP or high-profile patients.
  - b. Break the Glass Report: This report identifies users who have performed the Break the Glass function to access a patient record. The report must focus on incidents where "Other" is listed as a reason, or when the Break Glass function was used to access records of VIPs, employees or other high-profile patients.
  - c. Same Last Name Report: This report can help identify users who may have accessed their own patient record inappropriately or the medical records of family members without proper authorization.
  - d. User Print Job Report: A user who has printed far more patient records 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 Protected Health Information (PHI), Personally Identifiable Information (PII) and/or Payment Card Industry (PCI) cardholder data.
  - e. Remote Access Report: This report can help identify users who may be accessing the system remotely outside the scope of their job to avoid detection.
  - f. Guidelines for identifying risk to create other reports that must be evaluated for use in the Tenet monitoring program are listed in Attachment A, Guidelines for User Activity Monitoring.
5. Incident Reporting and Notification
 

All suspicious activity must be handled in accordance with EC.PS.01.01 Information Privacy and Security Incident Handling Standard.
6. For systems unable to meet this standard, a remediation plan must be in place in Compliance Matters and approved by the Corporate Information Security Department.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 8 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

#### IV. IMPLEMENTATION:

##### A. Information Privacy and Security Program

##### 1. Tenet Facility WITHOUT Regional Privacy Officer

- a. The Tenet Facility Compliance Officer, Tenet Facility Information Security Officer Tenet Facility Compliance Committee, and Tenet Facility Leadership Management are responsible for distribution and oversight of the Information Privacy and Security Program Standards at the facility level.
- b. Tenet Facility Leadership will:
  - (1) Adopt this standard and where necessary develop specific written procedures in order for the Tenet Facility to operationalize this standard;
  - (2) Develop appropriate methods to monitor adherence to the written procedures; and
  - (3) Report monitoring activity to the Tenet Facility Compliance Officer.


##### 2. Tenet Facility WITH Regional Privacy Officer

- a. The Regional Privacy Officer, Tenet Facility Information Security Officer, Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of Program Standards at the facility level.
- b. Tenet Facility Leadership, in coordination with the Regional Privacy Officer and Tenet Facility Compliance Committee will create specific policies and procedures as necessary in order for the Tenet Facility to operationalize the Program.
- c. Tenet Facility Leadership will report Program monitoring activity to the Regional Privacy Officer.

##### 3. Corporate Office (Dallas/Nashville)/Region/Market

- a. Tenet's Information Privacy/Security Office will work with the Tenet Facility Compliance Officers, , Tenet Facility PIRTS, Tenet Facility Information Security Officers Tenet Facility Compliance Committees, and Tenet Facility Leadership to develop, maintain,



	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.04</b>
	<b>Title:</b>  <b>ACTIVITY LOGS AND USER MONITORING STANDARD</b>	<b>Page: 9 of 9</b>
		<b>Effective Date: 08-31-17</b>
		<b>Retires Policy Dated: 10-27-16</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

and update policies, procedures and standards for protecting the privacy of PHI, PII, PCI cardholder data and other Confidential/Proprietary Information affording patients their rights with respect to their PHI, PII, PCI cardholder data.

- b. Tenet Corporate and Tenet Region/Market Offices must incorporate these standards into their specific policies and procedures where necessary.

## V. REFERENCES:

- EC.PS.01.00 Information Privacy and Security Administration Policy
- EC.PS.01.01 Information Privacy Security Incident Handling Standard
- EC.PS.04.00 Information Security Policy
- EC.PS.04.02 User Security and Conduct Standard
- Information Privacy & Security Glossary of Definitions
- Administrative policy AD 1.11 Records Management and its Record Retention Schedule

## VI. ATTACHMENTS:

- Attachment A: Guidelines for User Activity Monitoring

## **GUIDELINES FOR USER ACTIVITY MONITORING**

Audit log monitoring is required by the Security Rule Requirement at 45 C.F.R.

§164.308(a)(1)(ii)(D) Information System Activity Review:

A covered entity must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

To help understand and identify risks we must first know what PHI is available to users and how the security role limits access to the information. In setting up the strategy and process, we must also consider:

1. **Business Impact Assessment:** Determining possible business impacts to the Tenet Facility if the information were disclosed, integrity compromised or services disrupted.
2. **Threat and Risk Assessment:** Determining the risk (the chance) that identified threats could occur.
3. **Security Exposure Rating:** Evaluating the business impacts and the threats together to determine overall exposure to the Tenet Facility.

User activity monitoring is not simply a matter of randomly looking at activity; rather, it's an examination of events linked to specific users across multiple systems to develop a complete picture of what's going on. We monitor to:

1. **Prevent** – To prevent an incident/breach from ever occurring.
2. **Detect** – To determine if an incident/breach is occurring.
3. **Correct** – To ensure controls are effective after an incident/breach has occurred.

Potential risks to consider:

1. Does the system maintain or display social security numbers?
2. Does the system maintain or display "highly sensitive" information as defined in the Hospital's Notice of Privacy Practices (NPP)?
3. Do non-workforce members have access to your system?
4. Can the system send a fax?
5. Does the system log failed login attempts?
6. Does the system log print jobs?

Examples of risks include accessing/viewing:

1. The record of a patient with the same last name or address as the employee
2. VIP patient records (*e.g.*, board members, celebrities, governmental or community figures, physician providers, management staff, or other highly publicized individuals)
3. The records of those involved in high-profile events in the community (*e.g.*, motor vehicle accident, attempted homicide, etc.)
4. Patient files with isolated activity after no activity for 120 days
5. Other employee files across departments and within departments (organizations must set parameters to omit legitimate caregiver access)
6. Records with sensitive health information such as psychiatric disorders, drug and alcohol records, domestic abuse reports, and AIDS
7. Files of minors who are being treated for pregnancy or sexually transmitted diseases
8. Records of patients the employee had no involvement in treating (*e.g.*, nurses viewing patient records from other units)
9. Records of terminated employees (organizations must verify that access has been rescinded)
10. Portions of a record that an individual's discipline would not ordinarily have a need to access (*e.g.*, a speech pathologist accessing a pathology report)