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 shall 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 shall review certain audit log activities that occur on networks, systems, and applications to monitor potential risks.

A. Recording Audit Logs/Trails:

   An audit log/trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify when the event occurred, the UserID associated with the event, the program or command used to initiate the event, and the result.

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:

---

1 Replaces and retires Information Security policy Comp-Sec 8.2.2.
a. Intrusion activity
   (1) Failed login attempts with an invalid UserID
   (2) Failed login attempts with a valid UserID (password guessing attempts)
   (3) Failed password change attempts
   (4) Attempts to use privileges that have not been authorized

b. UserID administration activity
   (1) Modifications
   (2) Additions
   (3) Deletions
   (4) Disabling
   (5) Re-enabling
   (6) Changes to the privileges of users

c. System activity
   (1) Start-up
   (2) Shut-down

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. Perimeter Protection Logging Detail

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

a. Device activity

(1) Packet screening denials originating from trusted and untrusted networks
(2) User account management
(3) Modification of packet filters
(4) Application errors
(5) System errors
(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. Networks and applications must log activity using the following guidelines:

a. User activity should be logged at the field level, and shall record the following:

(1) UserIDs
(2) Access date/time
(3) User Access
(4) 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 should be maintained at the record level, and must record the following:

1. UserIDs
2. Action date/time
3. User Access
4. Record access
5. User Actions
6. Additions at the record level
7. Modifications at the record level
8. Deletions at the record level

c. If user activity cannot be logged at the record level, activity logging should be maintained at the system access level and this decision should 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. Attempted access to unauthorized data
7. Use of authorized advanced privileges (security bypass, etc)
8. Changes to critical application system files
9. Modifications
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 Security Standard**.

a. Logs must be rolled (a new log activated, the old log saved) rather than being overwritten (the same log is used again, losing data).

b. Log files are Confidential and must be protected such that no individual can modify or delete the logs.

c. Individuals authorized to view logs include members of the compliance staff, the internal audit staff, systems security staff, or systems management staff.

d. If an unauthorized individual needs access to these logs, they must request access in writing and obtain written permission from Tenet Facility Information Security Officer.

5. **Backup Retention**

Log files must be retained for a period of time so as to accomplish their purpose, and according to **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, use of a modem).
1. The designated Tenet Facility reviewer(s) for each information system must have knowledge of the workforce members’ roles in the organization and each workforce member’s current responsibilities.

2. All monitoring reports must be maintained in Compliance Central.

3. Unless required by law, monitoring reports for clinical systems must not be combined with a patient’s clinical record and shall 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 should 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).

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 should 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 shall be reported to the Tenet Facility Compliance Officer and Information security Officer and handled according to EC.PS.01.01 Information Privacy and Security Incident Handling Standard.
IV. IMPLEMENTATION:

A. Tenet Facility

1. The Tenet Facility Compliance Officer, Tenet Facility Information Security Officer and Tenet Facility Management are responsible for distribution and oversight of Information Privacy and Security Program Standards at the facility level.

2. Each Tenet Facility must
   a. Adopt this standard and where necessary develop specific written procedures in order for the Tenet Facility to operationalize this standard;
   b. Develop appropriate methods to monitor adherence to the written procedures; and
   c. Report monitoring activity to the Tenet Facility Compliance Officer.

B. Home Office

1. Tenet’s Information Privacy/Security Office will work with the Tenet Facility Compliance Officers, Tenet Facility Information Security Officers and Tenet Facility Management to develop, maintain, and update procedures and standards for protecting the privacy of PHI and other Confidential/Proprietary information and affording patients their rights with respect to their PHI.

2. Tenet Home Office and Tenet Regional 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 information/PHI is available to users and how the security role limits access to the information/PHI. In setting up the strategy and process, we should 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.

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 maintains or displays 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 should 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 should 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)