	Information Privacy and Security Program	No.	EC.PS.04.11
	Title: CYBERSECURITY POLICY	Page:	1 of 4
		Effective Date:	02/21/18
		Retires Policy Dated:	
		Previous Versions Dated:	

I. SCOPE:

This policy applies to (1) Tenet Healthcare Corporation and each of its wholly-owned subsidiaries and other 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 entity in which an Affiliate either manages or controls the day-to-day operations of the entity, in each case, as located in the United States. Tenet Healthcare Corporation, its Affiliates and the foregoing entities, organizations and hospitals are collectively referred to in this policy as "Tenet".

II. PURPOSE:

The purpose of this policy is to set forth general guidelines with respect to the establishment of procedures appropriate to identify and respond to incidents that may impact negatively the security, confidentiality, integrity or availability of Tenet Information Assets.

III. DEFINITIONS:

A. "Chief Information Security Officer" or "CISO" means the Tenet Information Systems department employee designated as responsible for the security of Tenet Information Assets from both internal and external threats.

B. "Cybersecurity Incident Response Plan" or "Plan" means the plan developed by the CISO, in collaboration with Tenet's Chief Information Officer and the Tenet Law Department, to respond to various incidents that may impact negatively the security, confidentiality, integrity or availability of Tenet Information Assets.

C. "Cybersecurity Incident Response Team" or "CIRT" means those Tenet employees designated with certain responsibilities in connection with the Cybersecurity Incident Response Plan and as identified therein.

D. "Personally Identifiable Information" shall be as defined by the National Institute of Standards and Technology.

E. "Protected Health Information" shall be as defined by the Health Insurance Portability and Accountability Act of 1996, as amended.

F. "Table-top Exercises" means discussion-based sessions where the CIRT members meet to discuss their roles and responses during various simulated incidents as specified by the CISO. The CISO or a facilitator designated by the CISO guides CIRT members through these exercises.

G. "Tenet Information Assets" means, without limitation, confidential information, proprietary information, Protected Health Information, and Personally Identifiable Information owned or maintained by Tenet, as well as computers, networks, electronic files, records, services hardware, and software, regardless of type or media and that is owned, leased, operated, used or controlled by or on behalf of Tenet.

IV. POLICY:

Tenet shall have in effect, implement, and update from time to time, processes, procedures, policies, standards and plans, including a Cybersecurity Incident Response Plan and Table-top Exercises and other assessments as deemed appropriate by the CISO, for identifying and responding to cybersecurity incidents that may affect Tenet Information Assets.

V. PROCEDURE:

A. The Cybersecurity Incident Response Plan shall include the following:

1. Identification of the CIRT, together with contact information, and responsibilities in the event of an incident.

2. Processes for determining the type of incident that has occurred.

3. Processes for determining how the incident occurred.

4. Processes for containment of the incident.

5. Calculation of the severity of the incident and associated risks.

6. Communication procedures.

7. Processes to remediate and recover from the incident.

8. Procedures to determine the means to avoid reoccurrence of the same or similar incident and identify any vulnerabilities.

B. The CISO shall conduct periodic Table-top Exercises.

C. The CISO shall annually assess the Cybersecurity Incident Response Plan and shall make changes necessary to update the Plan.

D. The CISO shall develop and implement communications to employees on an ongoing basis the means to report suspected or known security incidents.

E. Responsible Person

Tenet's Chief Information Officer is responsible for ensuring that all individuals adhere to the requirements of this policy, and that these procedures are implemented and followed at Tenet and that instances of non-compliance with this policy are reported to Tenet's Chief Compliance Officer.

F. 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. REFERENCES:

- AD 1.11 Records Management and its Record Retention Schedule

- EC. PS.01.00 Information Privacy and Security Administration Policy

--EC.PS.01.02 Breach Notification Standard for Unsecured Protected Health Information

--HR.ER W.03 Confidentiality of Company Information

--HR.ER W.18 Use of Information and Technology Systems

--Information Privacy & Security Glossary of Definitions: https://portal.etenet.com/departments/PrivacySecurity/Pages/Glossary%20of%20HIPAA%20Definitions.aspx

45 C.F.R. Parts 160 and 164

VII. ATTACHMENTS:

Not applicable.