INFORMATION PRIVACY AND SECURITY ADMINISTRATION STANDARDS

Information Privacy and Security Incident Handling Standard – The purpose of the standard is to provide an organized approach for reporting and responding to information security incidents as required under section 164.308(a)(6)(i) of the Security Rule. The growing use of external data communications at Tenet has increased the likelihood of encountering threats to the security of systems and information. A structured approach is needed to respond to information security incidents and return systems to normal operation as quickly as possible.

Breach Notification Standard – The purpose of this standard is to ensure that affected individuals, the media, and the Secretary of Health and Human Services (HHS) are appropriately notified of any Breach of unsecured protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and all applicable regulations and guidance.

Business Associate and Data Use Agreement Standard – The purpose of this Standard is to identify and define the standards for implementing contracting provisions related to those individuals and organizations identified as Business Associates.

Information Privacy and Security Risk Management Program Standard – The purpose of this standard is to provide guidance to management on certain administrative functions and to identify those responsible for controlling and monitoring those functions. Tenet's Information Security Policies and Procedures require certain administrative functions to ensure ongoing guarding of data integrity, confidentiality and availability.

Information Privacy and Security Contingency Planning Program Standard – The purpose of this standard is to provide requirements for contingency planning and guidelines for the components of the facility's data backup plan, business continuity plan (emergency mode of operations plan), and disaster recovery plan.

Disciplinary Guidelines Standard – The purpose of the standard is to establish a consistent procedure to be followed in circumstances where corrective, remedial, or disciplinary action is appropriate to address an employee or contractor's failure to comply with Tenet's Information Privacy and Security Program policies, Tenet's Standards of Conduct, applicable state privacy laws and federal privacy laws. These guidelines were designed to align a "typical" privacy violation with the "normal" disciplinary action consequences