TEMPLE UNIVERSITY HEALTH SYSTEM
HEALTH INFORMATION SECURITY AND PRIVACY COMPLIANCE PROGRAM

A SUPPLEMENT TO THE TEMPLE UNIVERSITY HEALTH SYSTEM COMPLIANCE PROGRAM

I. OUR FOUNDATION OF COMPLIANCE

A. MISSION, VISION AND VALUES: TEMPLE UNIVERSITY HEALTH SYSTEM (TUHS)

MISSION *(WHY WE EXIST)*

Our mission is to provide access to the highest quality of health care in both the community and academic setting.

VISION *(HOW WE ACHIEVE OUR MISSION)*

Our vision is to become the premier health system and the employer of choice in the Philadelphia Region.

VALUES *(OUR CONDUCT IN FULFILLING OUR MISSION AND VISION)*

- Respect
- Service
- Quality

It is necessary and important for all employees to be dedicated and loyal to Temple University Health System, Inc. ("TUHS"). In addition, it is expected that all members of the TUHS community be fiscally responsible, law abiding, honest, trustworthy, reliable, truthful and accurate in every manner of business conduct in order that TUHS may carry out its mission.

This policy extends this commitment to the obligation to protect and maintain all patient medical information with which TUHS is entrusted. As stewards of medical information, TUHS acknowledges and accepts all legal and regulatory obligations to maintain the privacy and confidentiality of protected patient health information. This underlying commitment is reflected in this supplement to the TUHS Corporate Compliance Program, which imposes Standards of Conduct upon each employee of the TUHS community.

B. PURPOSE OF THE CORPORATE COMPLIANCE PROGRAM

In 1996, the TUHS Board of Directors adopted the TUHS Billing Compliance Program (the Compliance Program), which included the Standards of Conduct to provide guidance

by which we will conduct ourselves in order to protect and promote integrity, and to enhance our ability to achieve our mission. The Compliance Program was revised in 2009 to its current form. This Program will assist us in carrying out our daily activities within appropriate ethical and legal standards. These obligations apply to our relationships with our patients, residents, physicians, third-party payers, subcontractors, independent contractors, vendors, consultants, and one another.

The Compliance Program is distributed periodically to all employees and annually to directors, officers, selected employees, volunteers, vendors and medical staff members having administrative or managerial responsibilities. Everyone is responsible to ensure that their behavior and activity is consistent with our Compliance Program by asking questions when unsure about what to do and reporting violations whenever they are discovered.

Our Compliance Program was developed to ensure that we must meet our ethical standards and comply with applicable laws, whether or not specifically mentioned in the Compliance Program or policies. Any questions regarding the existence, interpretation or application of the Compliance Program, regulations or laws should be addressed to the employee's supervisor or directly to the Corporate Compliance Officer. Inquiries may also be directed to the TUHS Compliance Hotline at (800) 910-6721.

C. LEADERSHIP RESPONSIBILITIES

While all individuals associated with TUHS are obligated to follow the Compliance Program, the leaders and supervisory personnel are expected to set an example for others to emulate. Leaders must ensure that those on their team have sufficient information to comply with laws, regulations, and policies, as well as the resources to resolve ethical dilemmas. They must help create a culture within their areas of responsibility that promotes the highest standards of ethics and compliance. This culture must encourage everyone within TUHS to raise concerns to those who have authority to address them. We must never sacrifice ethical behavior in pursuit of business objectives.

II. TUHS PATIENT HEALTH INFORMATION COMPLIANCE POLICY

Purpose of Policy and Regulatory Authority

This supplement to the TUHS Compliance Program establishes the standard for maintaining patient medical records while complying with all federal, state and local laws and regulations. It is not intended to supercede any of the various regulatory requirements that are currently operative. Rather, it is designed to create the requisite infrastructure within each TUHS facility to ensure compliance with the myriad of regulations concerning the maintenance, confidentiality and security of all patient information.

The operative standard for this TUHS Compliance Program Supplement is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Fair and Accurate Credit Transactions (FACT) Act of 2003. These federal laws apply to each facility within TUHS as an organized health care arrangement. This policy applies to all TUHS entities and Temple University entities that provide direct health care services hereinafter ("TUHS"). Accordingly, this document will establish the structure and policies required by these federal laws throughout TUHS.

III. TUHS HEALTH INFORMATION PRIVACY POLICY

A. MEDICAL RECORD PRIVACY COMMITTEE

1. Each TUHS covered entity shall create a privacy committee and appoint a privacy officer to chair their privacy committee.

2. The privacy officer shall be the designated individual within each facility to receive patient inquiries, complaints and requests from patients seeking to exercise control over their protected health information as detailed herein.

3. The privacy officers shall also be responsible for training their workforce members on the various components of these guidelines as well as providing regulatory revisions and updates as appropriate. Any revisions to policies or guidelines shall be reviewed and approved by the TUHS Privacy Officer to ensure consistency throughout TUHS.

4. The TUHS covered entity privacy committee shall consist of representatives from medical records, health information services, risk management, nursing and a representative from the professional staff.

B. COVERED INFORMATION

1. Health information is any information, whether oral or recorded in any form or medium, that:

    a. Is created or received by a health care provider, health plan, public health authority, employer, school or university, or health care clearinghouse; and

    b. Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an

individual, or the past, present or future payment for the provision of health care to an individual.

c. Is a subset of health information including individually identifiable health information (IIHI) which is health information created by a provider that identifies the individual patient or creates a reasonable basis to identify the individual patient.

d. Is "protected health information" (PHI): the IIHI which is transmitted maintained in either electronic medium or any other form. PHI includes the individual's designated record set which consists of medical, billing, enrollment, payment, or claims adjudication.

e. Is de-identified information: that which does not identify an individual or which there is no reasonable basis to believe that the information could be used to identify the individual. Such information will not use the individual's name, birth date, telephone number, social security number, medical record number or any other information from which the identity of the individual may be derived. Such information is not subject to the restrictions set forth herein.

C. DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI)

1. PHI disclosure is permitted when:

   a. Disclosed for purposes of treatment, payment or health care operations (TPO).

   b. Requested by the individual to which the PHI pertains.

   c. In the course of treatment of an emergency condition.

   d. When required by law, for public health or safety and health oversight activities, or in the case of death.

2. PHI may be disclosed without obtaining consent in the following situations:

   a. For public health activities, including but not limited to disease prevention or vital events reporting, child abuse or neglect, and Food and Drug Administration (FDA) reporting of adverse events, and/or dangerous/defective products.

b. Judicial and administrative proceedings pursuant to a subpoena, discovery request, or other lawful process as long as there is documentation that the individual has been notified and given the opportunity to object to the disclosure.

c. To coroners, medical examiners and funeral directors in the case of death.

d. For organ and tissue donation purposes.

e. To avoid a serious threat to health or safety or in an emergency.

f. For health oversight activities, including audits, investigations, inspections, licensure and disciplinary actions, civil, administrative or criminal proceedings, and the like, related to oversight of the health care system, government benefit and regulatory programs, and pursuant to civil rights laws.

g. TUHS may disclose a patient's PHI to another covered entity (i.e. one required to comply with federal privacy standards) that has a direct treatment relationship with the patient who is subject to the disclosure. The purpose of such disclosure, in addition to assuring continuity of care and/or coordination of benefits, may be for the detection of fraud or abuse, quality assessment/improvement, population-based activities relating to improving health or reducing health care costs, case management and care coordination, training, accreditation, licensing or credentialing activities.

h. Any such disclosure as listed above shall be accomplished through the release of the minimum necessary PHI to satisfy the purpose which triggered the request.

D. PATIENT'S INDIVIDUAL MEDICAL INFORMATION RIGHTS

1. Each TUHS Facility shall provide a Notice of TUHS Medical Record Privacy Practices that describes patient's individual rights with respect to PHI maintained by the covered facility. This TUHS Notice of Patient Rights shall be distributed to all patients and receipt of such notice shall be acknowledged by patients in writing on the first provision of medical services by TUHS.

2. This notice sets forth the TUHS Medical Record Policy and the individual patient rights with respect to their PHI.

3. These individual rights include:

a. The right to restrict the use and disclosure of PHI. Such requests must be in writing and the facility is not required to comply with the request, except for disclosures regarding services paid directly by the patient as long as the disclosure is not for treatment purposes. A decision to not comply with the patient's request must be in writing by the facility privacy officer and state the reason for the denial.

b. The patient has the right to inspect their records or obtain a copy by mail. Such requests must be in writing, and may be denied if the records are psychotherapy notes, are relevant to certain on-going research, were compiled in a civil or criminal investigation or proceeding, or were provided by a third party on the condition of confidentiality. The request may also be denied if access is reasonably likely to endanger or substantially harm the individual or another, in the professional judgment of a licensed health care professional. Denied requests must be in writing and describe the process by which the requesting individual may seek review or complain to the Secretary of Health and Human Services.

    1. Requests for access must be responded to within 60 days of receipt for on-site review and 90 days for off-site production.
    2. Copies will be provided at a reasonable charge.

c. An individual may request an amendment to their designated record set. Such a request must be in writing to the facility privacy officer and clearly state the reason for the request and the proposed amendment. The request may be denied if the facility did not create the PHI or the requested information would not be accessible to the individual for the reasons stated above. If upon review the facility privacy officer believes the existing data is accurate and complete, the request may be denied.

    1. The facility privacy officer may consult with the treating physician concerning any request by their patient to amend the medical records.
    2. Amendment requests must be responded to in writing within 90 days of receipt.
    3. The individual may file a written statement disagreeing with the denial, which may be rebutted by the facility. Both statements shall be appended to the individual's PHI.

d. An individual may request an accounting of disclosures of PHI related to the individual within the preceding six (6) years. Such an accounting does not include those disclosures made to persons involved in the individual's care, for payment purposes, or for health system oversight purposes. Such an accounting must be provided free of charge per twelve (12) month period with appropriate charges for all other accountings.

e. An individual right to notification in the event of an unauthorized disclosure resulting on a Breach as defined by HITECH regulations.

4. Any other contemplated disclosures of PHI not discussed above require individual patient authorization which must be specific to the purpose of the disclosure, and signed by the individual.

E. DISCLOSURES TO BUSINESS ASSOCIATES

1. A business associate is a person or organization which participates, performs or assists in performing:

   a. a function or activity involving the use or disclosure of PHI including claims processing, data management or analysis, utilization review, quality assurance, billing, practice management, or:

   b. legal, actuarial, accounting, consulting data aggregation, management, administrative, accreditation or financial services involving the use of PHI.

2. Contracts between TUHS and a business associate must:

   a. Establish the permitted uses and disclosures of PHI by the business associate.

   b. The business associate may not use or disclose the PHI in a manner that would violate the privacy requirements as set forth herein.

   c. The business associate may disclose the PHI for purposes required by law or to provide data aggregation services related to the health care operations of TUHS.

   d. The business associate may further disclose the PHI upon receipt of written reasonable assurances that the PHI will be held confidentially and used or further disclosed as required by law or for the purpose for which it was disclosed, and the business

associate will receive notice of any instance when the confidentiality is breached.

e. The business associate must also contract to use appropriate safeguards to prevent use or disclosure of the information other than as provided in the contract.

f. The covered facility must be notified of any use or disclosure of PHI not provided for by contract or permitted by law.

g. The business associate must also ensure that any agents or subcontractors to whom it provides PHI must agree to the same restrictions and conditions that apply to the business partner.

h. The business associate is subject to the Security Rule including administrative, technical and physical safeguards, policy and procedures, documentation and breach notification requirements.

IV. TUHS PATIENT HEALTH INFORMATION SECURITY POLICY

A. ADMINISTRATIVE PROCEDURES

1. All entities will maintain a data contingency plan which provide for:

   a. Data backup plan

   b. Disaster recovery plan

   c. Emergency mode operation plan

2. Written Policies documenting internal procedures for routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of Protected Health Information (PHI).

3. Maintain policies and procedures which establish:

   a. Rules for granting access to PHI

   b. Rules to determine a person's (or entities) initial right of access to a terminal, transaction, program, process or data.

   c. Rules governing modification of any person's (or entities) right of access to a terminal, transaction, program, process or data.

4. Establish a regular process of review and audit of the reports and logs of system access activity.

5. Establish written policies and procedures addressing the following personnel security clearance issues:

    a. Supervision of maintenance personnel by authorized supervisory personnel

    b. Maintenance of comprehensive and current records of all access authorizations

    c. Assuring that operating and maintenance personnel have proper access authorization for their level of responsibility

    d. Establishing the appropriateness of any individual's access to PHI

    e. Requiring all systems users, including maintenance personnel, to receive security awareness training regarding the use of PHI personnel

6. In order to assure a coherent, comprehensive and integrated enterprise-wide system of security each TUCE will develop:

    a. written security plans, rules, procedures, and instructions concerning all components of their security systems;

    b. written policies and procedures fro testing and verifying the security attributes of all new hardware and software, as well as periodic testing of the security attributes of existing hardware and software;

    c. a current formal inventory of all hardware and software assets;

    d. a formal process for functional testing, penetration and verification processes to determine that the security features of departmental systems are implemented as designed and are adequate for their environment;

    e. virus checking capabilities that identify and disable viruses.

7. Reports of potential breaches of security must be submitted pursuant to written policies and must include:

    a. documentation of reported security incidents;

b. responsive actions taken upon receipt of a security breach.

8. The Corporate Compliance and Privacy Officer will review security incidents to determine whether a Breach as defined by the HITECH regulations has occurred and issue any notifications needed.

V. TUHS IDENTITY THEFT PROTECTION POLICY

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the FACT Act of 2003. The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts."

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies and health care providers. A **covered account** is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions.

A. ADMINISTRATIVE PROCEDURES

1. All TUHS and TU entities will follow the procedure described below for the authentication of patient accounts. In emergency situations, medical treatment will be provided regardless of the patient's ability to provide documentation to substantiate his or her identity.

    a. The following documentation will be requested to prove identity:

        1. Driver's license or photo ID
        2. Medical Insurance Card

    b. If documentation is not available, patients with previous accounts will be asked to confirm their identity by stating at least two of the following identifiers:

        1. Correct spelling of the patient's first and last name.
        2. Date of birth
        3. Social security number
        4. Address
        5. Mother's maiden name

c. If the patient's information does not match a current account on file a new account will be created.

2. Identity Theft Red Flags

If identity cannot be established, then non-urgent appointments should be re-scheduled at the provider's discretion. The following situations will be considered Red Flags which require additional investigation:

a. No photo identification

b. Suspicious documentation

c. Incorrect spelling of first or last name

d. Address discrepancy

3. Response to Red Flags

Upon additional inquiry, either:

a. No further action will be necessary as the patient presented additional documentation to authenticate identity; or

b. When care is rendered with unresolved issues remaining, the file will be forwarded to an immediate supervisor for resolution. The supervisor will alert the Department of Revenue Cycle (or other accounting office as appropriate) to place a hold on the account until the investigation is completed. The department head will contact the CCO with the investigation results. The investigation may result in notification to the identity theft victim as determined by the CCO.

4. Reports of Identity Theft Post Billing

a. When a potential incident of identity theft is identified post billing, department heads will forward the incident to the Department of Revenue Cycle (or other accounting office as appropriate) for investigation. The Department of Revenue Cycle (or other accounting office as appropriate) will report the investigation results to the CCO**.**

b. Individuals will be required to provide documentation in support of their claim of identity theft.

c. Individuals claiming identity theft will be advised that they should file a complaint with the FTC and place a "Fraud Alert" with the three major credit bureaus.

d. Once identity theft has been verified, the effected entity will handle the correction of medical records. The CCO will contact the identity theft victim and make other required disclosures in the event identity theft is confirmed.

VI. BREACH NOTIFICATION PROCEDURES

The Omnibus final rule, entitled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health (HITECH) Act" requires covered entities to notify patients of a breach of their unsecured PHI.

Under the Omnibus Rule there is a presumption that an unauthorized use or disclosure of unsecured PHI constitutes a "breach of unsecured PHI" unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised. All incidents of potential unauthorized access are investigated by the CCO. If an unauthorized disclosure is confirmed the CCO will consider the following factors to determine the probability that the PHI has been compromised.

a. The nature and extent of PHI involved in the use or disclosure, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized entity to whom the PHI was disclosed or who used the PHI; whether the PHI was actually acquired or viewed.

c. The extent to which the risk to the PHI has been mitigated.

The CCO will evaluate the information gathered during the investigation to determine whether there is objective evidence that there is a low probability that the PHI has been compromised. In the event that the disclosure is determined to be a breach of unsecured PHI, the CCO will take the following actions.

a. Notify the patient in writing of the nature of the incident, the type of PHI that was compromised, what was done to mitigate the issue and what the patient can do to protect themselves no later than 60 days following the discovery of a breach.

b. Enter the incident in the HIPAA incident report log to be reported to the HHS Secretary at the end of the calendar year, unless the breach involves 500 or more individuals.

c. Breaches of unsecured PHI involving 500 or more individuals require patient, agency and media notifications no later than 60 days following the discovery of a breach.

d. Recommend mitigating measures including disciplinary action and re-education.

Failure to adhere to these procedures or any of the applicable laws, regulations or Rules will be considered a violation of the TUHS Standards of Conduct that may result in appropriate disciplinary action. Any questions concerning this Program should be directed to the appropriate TUHS facility privacy officer or the TUHS Privacy Officer. Reports may also be directed anonymously to the TUHS Compliance Hotline at (800) 910-6721.

Submitted for approval to the TUHS Audit and Compliance Committee on June 13, 2013.