Austin/Travis County
Health and Human Services Department

HIPAA/PII/PCI-DSS Compliance Improvement Plan

2015-2016

Approved:
Director: 4/29/2015

Chief Administrative Officer:

Records Management Administrator: 4-29-15

Health IT Manager: 4-29-15

Quality Improvement Plan

I. Purpose and Scope

Introduction: The Austin/Travis County Health and Human Services Department, (A/TCHHSD) is committed to ensuring the confidentiality, integrity and availability of protected records and information (data) by developing and sustaining a Quality Improvement (QI) plan related to risk management.

Vision: To meet or exceed all regulatory compliance requirements related to Protected Health Information (PHI), Personally Identifiable Information (PII), and Payment Card Industry Data Security Standards (PCI-DSS).

Mission: To ensure protection of health information and individually identifiable information maintained by A/TCHHSD by implementing best practices (ISO, NIST, COBT, etc.) for risk management and security controls..

Authority and Accountability:
The Department Director provides the authority for the functions of the HIPAA, PII, and PCI-DSS Compliance QI Committee. Executive, Division, and Unit/Program Managers are responsible for identification of HIPAA, PII, and PCI-DSS protected information within their purview and for implementation of appropriate security controls.

1. The HIPAA, PII, and PCI-DSS Compliance QI Committee will develop and maintain a method for A/TCHHSD management to assess the level of compliance with regulations related to protected data that A/TCHHSD is responsible for.
2. Facilitate implementation of appropriate risk management measures related to privacy or security controls.

Scope:
The scope of the HIPAA, PII, PCI-DSS Compliance QI Committee's work encompasses all PHI, PII, PCI within A/TCHHSD and includes the following activities performed both independently and jointly with unit/program working teams, as deemed appropriate:

1. Determine type and location of protected data.
2. Determine regulatory compliance required for protected data.
3. Determine risk associated with protection of sensitive data.
4. Identify gaps in privacy or security controls related to protected data.
5. Develop a mitigation strategy to implement missing controls.
6. Review, monitor, track progress, and report on the HIPAA, PII, PCI-DSS Compliance QI plan

Purpose:
The A/TCHHSD is committed to delivering optimal and quality public health services and programs to the community in collaboration with our partners and stakeholders. These quality services and programs are aligned with the department wide Strategic Priorities, Goals and Objectives.

The Continuous Quality Improvement (CQI) executive leadership team, senior team, division, unit and program levels will use a variety of activities to ensure that quality services are being provided to the community.
These include:

1. On-going evaluation of processes for effectiveness
2. Report on potential problems and quality improvement opportunities
3. Subsequent process improvements and problem resolution
4. Monitoring and documenting Quality Improvement data outcomes of implemented changes
5. Communicating and sharing lessons learned and knowledge gained through the CQI process

Objectives:

1) Create an environment and organizational culture where staff is involved and knowledgeable regarding the protection and security of protected records and information (data).
2) Facilitate activities of a working team in each unit/program to continuously monitor and evaluate compliance and mitigation issues related to protected records and data; and to identify opportunities to improve compliance and protection of records and data. This includes but is not limited to the following;
    1. Identification of protected records and data
    2. Inventorying standards, policies, and procedures
    3. Identifying resources and providing workforce development opportunities for staff related to HIPAA, PII, and PCI-DSS training (type, level, occurrence, tracking, etc.)

II. HIPAA/PII/PCI-DSS Compliance Quality Improvement Committee

Composition: The HIPAA, PII, and PCI-DSS Quality Improvement Committee is composed of the following:

1. Chief Administrative Officer
2. Department Privacy Officer
3. Health Information Technology Manager
4. Internal Auditor
5. Unit Privacy Officers

Scheduled Meetings: The committee will meet quarterly to address training needs, issues/challenges related to HIPAA, PII, and PCI-DSS compliance, and to evaluate the status of overall program monitoring.

Confidentiality: The HIPAA, PII, and PCI-DSS Compliance QI Committee will maintain confidentiality of documentation and information as appropriate. It is the responsibility of the program committee to determine what data is gathered and how it should be preserved.

Responsibilities of the Committee:

The HIPAA, PII, and PCI-DSS Committee Members are responsible for the following;

1. Chief Administrative Officer
   - Executive oversight
   - Support of overall program (budget needs, ELT support, etc.)

2. Records Management Administrator (Privacy Officer)
   - Execution of the compliance plan with support from all other committee members
   - Chair/facilitate quarterly committee meetings
   - Assist in the identification of departmental risk related to HIPAA, PII, and PCI-DSS
   - Assist in the development of policies and procedures related to HIPAA, PII, and PCI-DSS

3. Health IT Manager (Security Officer)
   - Providing support to the compliance in all areas related to systems and data management
   - Assisting in the identification of departmental risk related to HIPAA, PII, and PCI-DSS
   - Develop mitigation strategy including security controls

4. Internal Auditor
   - Assist and advise A/TCHHSD management in identifying departmental risk related to HIPAA, PII, and PCI-DSS
   - Communication of risks identified in audit projects to the HIPAA, PII, and PCI-DSS Compliance Committee
   - Provide monitoring of overall plan compliance with standards and policies and procedures related to protected data

5. Unit Privacy Officers
   - Attending quarterly committee meetings scheduled by the Department Privacy Officer

- Working closely with committee to identify type and location of protected records and information (data)
- Working closely with committee to help identify departmental risk related to HIPAA, PII, and PCI-DSS
- Communicate to unit staff information learned from quarterly HIPAA, PII, and PCI-DSS compliance meetings
- Establishing criteria on what information is minimally necessary to be communicated either within the Department, the Divisions, or to a third party.
- Working with the Privacy Officer in the ongoing evaluation of the department's privacy policies and procedures to ensure full compliance with all state and federal patient privacy laws.
- Immediately notify the Department's Privacy Officer of any client privacy complaint or concern and work with the unit's management and Human Resources, if appropriate, to investigate the matter.
- Reporting the unit/program's progress as described below.

III. HIPAA, PII, and PCI-DSS Compliance QI Monitoring and Evaluation

Monitoring Status:

The Committee will track and monitor the status of unit/program working teams' progress in identifying HIPAA, PII, and PCI-DSS data and records, and implementation of appropriate security controls. A tracking and reporting tool will be developed by the Committee for use by each working team to report progress and activities each quarter.

Each unit/team will report their compliance with the standards and policies and procedures periodically and compare them to relevant compliance requirements and best practices.

The *HIPAA, PII, PCI Summary Report* will be due to the Department Privacy Officer on the 15th of the scheduled month.

Data Sources: Information needed to evaluate compliance relative to standards set by the HIPAA, PII, and PCI-DSS Committee. Data comes from many areas including the following: medical and program records; organizational policies and procedures; meeting minutes; training logs and sign-in sheets; customer feedback, and relevant standards.

Minutes:

Minutes will be taken for all HIPAA, PII, and PCI-DSS Compliance QI Committee meetings. These minutes will be distributed after each meeting for review; corrections and follow up on action items.

Definitions

Continuous Quality Improvement (CQI) – Quality improvement in public health is the use of a deliberate and defined improvement process, such as Plan-Do-Check-Act, which is focused on activities that are responsive to community needs and improving population Health.

Health Insurance Portability and Accountability Act (HIPAA) – Federal law that provides protections for individually identifiable health information held by covered entities and their business associates and gives patients' rights with respect to that information. It also specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. (To include Texas House Bill 300)
http://www.hhs.gov/ocr/privacy/index.html

PCI Data Security Standard – A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI Data Security Standard is comprised of 12 general requirements designed to: Build and maintain a secure network; Protect cardholder data; Ensure the maintenance of vulnerability management programs; Implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies.
https://www.pcisecuritystandards.org/faq/

Personally Identifiable Information (PII) – Any information created, collected or maintained by the City of Austin that can be used to uniquely distinguish, trace or link to an individual's identity. Examples may include name, social security number, date and place of birth, a mother's maiden name or biometric records. Other information may also include personal, medical, educational, financial and employment information.

Protected Health Information (PHI) – Generally individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care

to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. PHI excludes individually identifiable health information in: (i) education records covered by the Family Education Rights and Privacy Act (20 U.S.C. 1232g); (ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) employment records held by a covered entity in its role as employer [45 CFR § 160.103].
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm?mobile=nocontent
http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a2.htm

Protected Records and Information (Data) – Records and Information that contain PII and/or that is protected by HIPAA.