Subject: Administrative, Technical, and Physical Safeguards

Objective:

I. To ensure that Health Share/Tuality Health Alliance (THA) has established criteria for the safeguarding of confidential information and to minimize the risk of unauthorized information access, use, or disclosure.

Policy:

I. General Overview of Information Mediums

THA must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of privacy policies. Information to be safeguarded may be in any medium, including paper, verbal, visual, electronic formats, and may be shared through mail.

a. *Paper Format*
   - Each THA workstation will store files and documents in locked rooms or storage systems.
   - In workstations where lockable storage is not available, THA staff must take reasonable efforts to ensure the safeguarding of confidential information.
   - Each THA workstation will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
   - Each THA staff person will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

b. *Verbal Format*
   - THA staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
   - THA staff shall speak quietly or schedule an enclosed office and/or interview room for the verbal exchange of confidential information.
     - **Exception:** In work environments structured with few offices or closed rooms, such as in THA or open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that THA has met the reasonable safeguards and minimum necessary requirements.
   - THA staff must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

Subject: Administrative, Technical, and Physical Safeguards

c. *Visual Format*
   - THA staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
     - Computer screens: THA staff must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
     - Paper documents: THA staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

d. *Computer/Electronic Format*
   - THA staff who are assigned to use computers are responsible for maintaining the security of passwords or other access methods according to THC policy HR-33.

e. *Mail*
   - Each THA employee will ensure that mail is prepared accurately for delivery.
   - Outgoing mail must include a complete sending address, including first and last name of recipient, agency name, and complete street and city address. If printed labels are not used, write or print legibly.
   - The outgoing mail must also include a complete return address (first and last name of sender, agency, complete street and city address).

II. Safeguarding Confidential Information

a. Implementation of levels of access and the use/disclosure of minimum necessary information will promote administrative safeguards.
   - Levels of access are a form of security allowing access to data based on job function in accordance with THC Operational policies and procedures.
   - Employees shall be assigned to a level of access per their job descriptions, allowing access only to the minimum necessary information to fulfill job functions.

b. The THA Privacy Officer and members from the HIPAA taskforce will provide ongoing education on THA Safeguards of PHI and may conduct periodic reviews in order to evaluate and improve the effectiveness of their current safeguards.

c. Development and implementation of department-wide security policies will enhance administrative safeguards.
   - THA staff will be required to sign a document that constitutes a formal commitment to adhere to the department-wide security policies.

Subject: Administrative, Technical, and Physical Safeguards

d. *Off-Site Work Practices*
   - All the safeguard requirements for the workplace apply equally to any use of confidential information away from the THA workplace. Files and records should be securely transported.
   - THA staff authorized to use laptop computers off-site are responsible for assuring the security, as well as minimized risk of loss, of the device and its contents.
     - THA staff working on non-work shared computers should observe security protocols to prevent unauthorized users from accessing confidential information.
   - THA staff should ensure care when using telephones outside of the work space. Cell phones, Blackberry or other telephones require care to protect confidential information.
     - THA staff should avoid using identifiable information about members unless staff has taken reasonable efforts to assure the privacy of the call.

References: DMAP Policy AS-100-05: Administrative, Technical, and Administrative Safeguards
Health Share RAE Participation Agreement
THC Policy O-097G: Health Information Safeguards
THC Policy HR-33: Communication Technology Usage

Formulated: March 7, 2003

Reviewed: September 2013
September 2015

Revised: November 2007
October 2010

Formulated:	March 2003
Reviewed:	September 2013 September 2015
Revised:	November 2007 October 2010