HILL COUNTRY COMMUNITY ACTION ASSOCIATION INC.

Information Security and Privacy Policies and Procedures

INTRODUCTION

The protection of client confidentiality is a core value of Hill Country Community Action Association (HCCAA). HCCAA is required by law and professional ethics to protect the confidentiality and integrity of client information.

PURPOSE

The purpose of these Policies applies with respect to the use and disclosure of confidential information on the premises of or in the custody of Hill Country Community Action Association. Confidential Information means any client communication or record (whether oral, written, electronically stored or transmitted, or in any other form).

As a non-profit corporation established under the Texas Non-Profit Corporation Act, Article 1396-01 et seq., Vernon's Texas Civil Statutes, HCCAA does not have as its primary purpose the provision of or payment for health care services.

POLICIES

HCCAA will establish, implement and maintain appropriate procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of Confidential Information, and with respect to Personal Health Information (PHI), as described in the HIPAA Privacy and Security Regulations, or other applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as HCCAA has such Confidential Information in its actual or constructive possession.

HCCAA will exercise reasonable care to protect confidential information to the same degree of care it uses to protect its own confidential, proprietary and trade secret information to prevent any portion of the confidential information from being used in a manner that is not expressly an authorized purpose or as required by law.

HCCAA will appoint a Privacy Official and an Information Security Official to establish procedures that will oversee the confidentiality and personal policy that this agency has set in place, give notice of our legal duties and privacy practices regarding confidential client information and protected health information about clients, and follow the terms of our notice that is currently in effect. All workforce members in the agency that provides one-on-one assistance with clients will comply with the PHI standards established in this policy.

All staff members of HCCAA's workforce shall be familiar with and shall comply with this Policy. Workforce may not use, disclose or request clients' health information except as permitted or required by this Policy.

This policy applies with respect to confidential client information and protected health information on the premises of or in the custody of HCCAA.

Each Department of HCCAA may adopt additional implementation procedures as appropriate in order to promote compliance with this Policy. Additional implementation procedures of individual Departments may not require a lesser level of privacy protection or otherwise be contrary to or inconsistent with these Policy and Procedures.

HCCAA will not disclose or allow access to any portion of the confidential information to any person or other entity, other than authorized HCCAA Workforce or Subcontractors who have been trained and understand the importance of confidentiality, privacy, security and of promptly reporting any event or breach to HCCAA's management.

HCCAA will establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractors who fails to comply with these Policies and Procedures.

HCCAA will not disclose or provide access to any confidential information, except on the basis that such act is required by law, without notifying either the Contractor or HCCAA's legal counsel to determine whether HCCAA should object to the disclosure or access and seek appropriate relief. HCCAA will maintain an accounting of all such requests for disclosure and responses and provide such accounting to the Contractor within 48 hours of the Contractor's request.

HCCAA will not attempt to re-identify or further identify confidential information or de-identify information, or attempt to contact any individual whose records are contained in the confidential information, except for an authorized purpose without express written authorization from the Contractor or as expressly permitted by a Contract.

HCCAA will not permit, or enter into any agreement with a Subcontractor to create, receive, maintain, use, disclose, have access to or transmit confidential information on behalf of HCCAA without assurance that the Subcontractor has adequate safeguards in place to protect confidential information.

HCCAA is directly responsible for compliance with, and enforcement of, all conditions for creation, maintenance, use, disclosure, transmission and destruction of confidential information and the acts or omissions of Subcontractors as may be reasonably necessary to prevent unauthorized use.

HCCAA will maintain confidential information in a Designated Record Set.

HCCAA will make confidential information available to Contractors in a Designated Record Set upon request.

HCCAA will provide Personal Health Information (PHI) to an Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations.

HCCAA will release PHI in accordance with the HIPAA Privacy Regulations upon receipt of a valid written authorization.

HCCAA will make other Confidential Information in its possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach of Unsecured PHI as defined in HIPAA. HCCAA will maintain an accounting of all such disclosures and provide it to Contractors within 48 hours of Contractors' request.

HCCAA will document and make available to Contractors the PHI required to provide access and accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations.

HCCAA will respond to a request for access, amendment or accounting of PHI from an individual with a right of access to information subject to these Policies and in compliance with the HIPAA Privacy Regulations. HCCAA will maintain an accounting of all responses to requests for access to or amendment of PHI and provide it to Contractors within 48 hours of Contractors' request**.**

HCCAA will provide, and will cause its Subcontractor and agents to provide, to Contractors periodic written certifications of compliance with controls and provisions relating to information privacy, security and breach notification, including without limitation information related to data transfers and the handling and disposal of Confidential Information.

HCCAA, except as otherwise limited by these Policies and Procedures applicable to the Confidential Information, may use or disclose PHI for the proper management and administration of the Agency or to carry out the Agency's legal responsibilities if:

(1) Disclosure is required by law;

(2) Reasonable assurances are obtained from the Person to whom the information is disclosed and that person will:

(a) Maintain the confidentiality of the Confidential Information in accordance with these Policies and Procedures;

(b) Use or further disclose the information only as required by Law or for the authorized purpose for which it was disclosed to the person; and

(c) Notify HCCAA of any event or breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence.

Except as otherwise limited by these Information Security and Provacy Policies and Procedures, HCCAA will, if requested by Contractors to comply with law, use PHI to provide data aggregation services to Contractors, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by HIPAA.

HCCAA will, on the termination or expiration of any Data Use Agreement or Base Contract with a Contractor, at its expense, send to Contractor or Destroy, at Contractor's election, and to the extent reasonably feasible and permissible by law, all Confidential Information received from Contractor or created or maintained by HCCAA or any of HCCAA's agents or Subcontractors on Contractor's behalf if that data contains Confidential Information. HCCAA will certify in writing to Contractor that all the Confidential Information that has been created, received, maintained, used by or disclosed to HCCAA, has been destroyed or sent to Contractor, and that HCCAA and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, HCCAA will acknowledge and agree that it may not destroy any Confidential Information if federal or state law, or Contractor record retention policy or a litigation hold notice prohibits such Destruction. If such delivery or destruction is not reasonably feasible, or is impermissible by law, HCCAA will immediately notify Contractors of the reasons such delivery or destruction is not feasible, and agree to extend indefinitely the protections of these Policies and Procedures to the Confidential Information and limit its further uses and disclosures to the purposes that make the return delivery or destruction of the Confidential Information not feasible for as long as HCCAA maintains such Confidential Information.

HCCAA will create, maintain, use, disclose, transmit or destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses**.**

If HCCAA accesses, transmits, stores, and/or maintains Confidential Information, HCCAA will comply with periodic security controls compliance assessment and monitoring by Contractor as required by state and federal law, based on the type of Confidential Information HCCAA creates, receives, maintains, uses, discloses or has access to and the authorized purpose and level of risk.

HCCAA's security controls will be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. HCCAA will update its security controls assessment whenever there are significant changes in security controls for Confidential Information and will provide the updated document to Contractors upon request.

HCCAA will designate and identify a person as Privacy Officer and Information Security Officer, who is authorized to act on behalf of HCCAA and is responsible for the development and implementation of the privacy and security requirements in these Policies and Procedures.

HCCAA employees will have access to Confidential Information solely to the minimum extent necessary to accomplish the Agency's business, and further, that each is bound by HCCAA Policies related to Client Confidentiality.

HCCAA will make available to Contractor any information Contractor requires to fulfill Contractor's obligations to provide access to, or copies of, PHI in accordance with HIPAA and other applicable laws and regulations relating to Confidential Information. HCCAA will provide such information in a time and manner reasonably agreed upon.

HCCAA will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form.

(1) A secure transmission of electronic Confidential Information *in motion* includes secure File Transfer Protocol (SFTP) or Encryption at an appropriate level or otherwise protected as required by rule, regulation or law.

(2) Confidential Information *at rest* requires Encryption unless there is adequate administrative, technical, and physical security, or as otherwise protected as required by rule, regulation or law.

(3) All electronic data transfer and communications of Confidential Information will be through secure systems.

HCCAA will provide proof of system, media or device security and/or Encryption to Contractor no later than 48 hours after Contractor's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. De-identification of Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance.

HCCAA will comply with the following laws and standards if applicable to the type of Confidential Information and HCCAA's Authorized Purpose:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;
- OMB Memorandum 07-16;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as defined in the DUA;
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI; and
- Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that HCCAA supports on behalf of HHS.

PROCEDURES

PRIVACY STAFF AND RESPONDIBILITIES

The appointed Privacy Officer and Information Security Officer will oversee the confidentiality and personal policy that this agency has set in place, give notice of our legal duties and privacy practices regarding confidential client information and protected health information about clients, and follow the terms of our notice that is currently in effect.

1. Privacy Official.
   a. The Chief Operating Officer will perform the duties of the Privacy Official.
   b. The Privacy Official shall:
      i. Develop, implement, maintain, and monitor privacy policies and procedures pertaining to individually identifiable health information
      ii. Serve as a key privacy advisor for clients, handle disputes and manage client's requests regarding their records.
      iii. Serve as a contact person to provide information about matters covered by HCCAA's notice of privacy practices and shall be responsible for receiving complaints related to client privacy matters.
      iv. Periodically report progress and developments related to the compliance activities of the Privacy Officer to the executive administration of HCCAA.

2. Information Security Official.
   a The Agency's Technology Manager will perform the duties of the Information Security Official.
   b The Information Security Officer shall:
      i. Work with all workforce members of HCCAA in ensuring that security polices and procedures are maintained.
      ii. Be responsible and accountable for all activities related to the security of electronic protected information.
      iii. Review and establish all system related information security plans throughout the organization to ensure alignment between security and privacy practices.
      iv. Work with the Chief Executive Officer to enforce a disciplinary system of sanctions for failure to comply with security policies for all employees and constituents of the organization.
      v. Work with all facilities and departments to standardize policies and procedures in regards to the security of confidential information.
      vi. Organize the development and requirement for all workforce members to use a Fax Cover Sheet containing a confidentiality statement on all documents faxed to external departments and/or business associates.
      vii. Organize the development and requirement for all workforce members to insert email disclaimer language to their auto signature on all email messages containing confidential information.
      viii. Perform other activities as assigned.

3. Workforce.
   a. All members of the HCCAA workforce providing one-on-one assistance to clients that involves confidential information shall:

i. Provide at first visit a Release of Information Form.
i. Safeguard and secure all documents containing confidential information.
ii. Ensure confidential statement is on all fax cover sheets when faxing documents.
iii. Ensure a confidential statement is included on all email messages containing confidential information.

BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

1. HCCAA will cooperate fully with Contractors in investigating, mitigating to the extent practicable and issuing notifications directed by Contractors, for any Event or Breach of Confidential Information to the extent and in the manner determined by Contractors.

2. HCCAA'S obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the Event are mitigated to Contractor's satisfaction.

3. Breach Notice:

   Initial Notice. For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after Discovery, or in a timeframe otherwise approved by Contractor in writing, initially report to Contractor's Privacy and Security Officers and division responsible for the DUA; Report all information reasonably available to HCCAA about the Event or Breach of the privacy or security of Confidential Information; Name, and provide contact information to Contractors for, HCCAA's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

   48-Hour Formal Notice. No later than 48 consecutive clock hours after Discovery, or a time within which Discovery reasonably should have been made by HCCAA of an Event or Breach of Confidential Information, provide formal notification to to Contractor's Privacy and Security Officers and division responsible for the DUA including all reasonably available information about the Event or Breach, and HCCAA's investigation, including without limitation and to the extent available:

   a. The date the Event or Breach occurred;
   b. The date of HCCAA's and, if applicable, Subcontractor's Discovery;
   c. A brief description of the Event or Breach; including how it occurred and who is responsible (or hypotheses, if not yet determined);
   d. A brief description of HCCAA's investigation and the status of the investigation;
   e. A description of the types and amount of Confidential Information involved;
   f. Identification of and number of all Individuals reasonably believed to be affected, including first and last name of the individual and if applicable the, Legally authorized representative, last known address, age, telephone number, and email address if it is a preferred contact method, to the extent known or can be reasonably determined by HCCAA at that time;
   g. HCCAA's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or a DUA for Contractor's approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;
   h. HCCAA's recommendation for Contractor's approval as to the steps Individuals and/or HCCAA on behalf of Individuals, should take to protect the Individuals from potential harm, including without limitation HCCAA's provision of notifications, credit protection, claims monitoring, and

any specific protections for a Legally Authorized Representative to take on behalf of an Individual with special capacity or circumstances;

i. The steps HCCAA has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);
j. The steps HCCAA has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Event or Breach;
k. Identify, describe or estimate the Persons, Workforce, Subcontractors, or Individuals and any law enforcement that may be involved in the Event or Breach;
l. A reasonable schedule for HCCAA to provide regular updates to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by Contractor, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and
m. Any reasonably available, pertinent information, documents or reports related to an Event or Breach that Contractor requests following Discovery.

INVESTIGATION, RESPONSE AND MITIGATION

1. HCCAA will immediately conduct a full and complete investigation, respond to the Event or Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to Contractor for incident response purposes and for purposes of Contractor's compliance with report and notification requirements, to the satisfaction of Contractor.
2. HCCAA will complete or participate in a risk assessment as directed by Contractor following an Event or Breach, and provide the final assessment, corrective actions and mitigations to Contractor for review and approval.
3. HCCAA will fully cooperate with Contractor to respond to inquiries and/or proceedings by state and federal authorities, Persons and/or Individuals about the Event or Breach.
4. HCCAA will fully cooperate with Contractor's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Event or Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by Contractor in a Corrective Action Plan if directed by Contractor under Contract.

BREACH NOTIFICATION TO INDIVIDUALS AND REPORTING TO AUTHORITIES

1. HCCAA will provide Breach notification to Individuals, regulators or third-parties, as specified by Contractor following a Breach.
2. HCCAA must obtain Contractor's prior written approval of the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in HCCAA's name and on HCCAA's letterhead, unless otherwise directed by Contractor, and will contain contact information, including the name and title of HCCAA's representative, an email address and a toll-free telephone number, if required by applicable law, rule, or regulation, for the Individual to obtain additional information.
3. HCCAA will provide Contractor with copies of distributed and approved communications.
4. HCCAA will have the burden of demonstrating to the satisfaction of Contractor that any notification required by Contractor was timely made. If there are delays outside of HCCAA's control, HCCAA will provide written documentation of the reasons for the delay and will request Contractor to cooperate and assist with HCCAA's information requests in order to make such notifications and reports available as soon as reasonably possible.

INSURANCE

.

1. HCCAA will maintain commercial insurance with policy limits in an amount sufficient to cover HCCAA's liability arising under a Data Use Agreement and under which policy the Contractor is a beneficiary.
2. HCCAA will provide the Contractor with written proof that required insurance coverage is in effect, at the request of the Contractor.

FEES AND COSTS

Except as otherwise specified in a DUA or Contract, including but not limited to requirements to insure and/or indemnify the Contractor, if any legal action or other proceeding is brought for the enforcement of a DUA, or because of an alleged dispute, contract violation, Event, Breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of a DUA, HCCAA will bear only its legal expenses and the other cost incurred in that action or proceeding.

DEFINITIONS

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to HCCAA or that HCCAA may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following:

(1) Client Information;

(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;

(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

(4) Federal Tax Information;

(5) Personally Identifiable Information;

(6) Social Security Administration Data, including, without limitation, Medicaid information;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Covered Entity" means a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

"Data Use Agreement" is required before a covered entity may use or disclose a limited data set and provides a covered entity with satisfactory assurance that the limited data set recipient will only use or disclose the PHI for limited purposes.

"HIPAA Privacy Standards" means the Standards for the Privacy of Individually Identifiable Health Information, which is part of the Privacy Laws.

"HIPAA Transactions" are those categories of electronic transactions that are regulated by the HIPAA Final Electronic Standard Transactions and Code Sets.

"Individual" means the person who is the subject of PHI.

"Information Security Official" performs ongoing information risks assessments and audits to maintain the confidentiality, integrity and availability of healthcare information required by HIPAA.

"Legally Authorized Representative" of the Individual, as defined by Texas law, including as provided in 45 CFR 435.923 (Medicaid); 45 CFR 164.502(g)(1) (HIPAA); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; Estates Code Ch. 752 and Texas Prob. Code § 3.

"Limited Data Set" is PHI that excludes the following direct identifiers of the individuals or of relatives, employers, or household members of the Individuals: (i) names; (ii) postal address information other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) e-mail addresses; (vi) Social Security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal Resource Locators

("URLs"); (xiv) Internet Protocol ("IP") address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images. Identifiable information that may remain in a limited data set includes dates relating to a client (dates of service, admission, or discharge; date of birth; date of death) and information relating to the town or city, state, and five-digit zip code of the client, his or her employer, and the client's household members.

"Privacy Official" is the Agency privacy/client information officer.

"Protected Health Information or "PHI" is individually identifiable health information that is transmitted or maintained in any medium or form. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended; in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv) (student treatment records excepted from FERPA); and in employment records held by a covered entity in its role as an employer.

"Required by law" means a mandate contained in law that compels HCCAA to make a use or disclosure of PHI and is enforceable in a court of law. "Required by law" includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the Medicare program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

"Sanctions" are administrative actions by a covered entity taken against members of its workforce who fail to comply with the entity's policies and procedures or with the requirements of the Privacy Standards.

"Workforce" includes all employees of HCCAA. Workforce also includes non-employees who are under Hill Country Community Action Association's direct control, including students, visiting faculty, volunteers, residents and trainees. Workforce may include, if so designated in the discretion of Hill Country Community Action Association, any contractors who have a workstation on Hill Country Community Action Association's premises, such as a temporary employee or an information technology contractor who works on site on Hill Country Community Action Association's information systems.