Cook Inlet Tribal Council, Inc.

POLICY:	**INFORMATION TECHNOLOGY DEPARTMENT HIPAA PRIVACY AND COMPLIANCE**	**POLICY NO.**	**2.200**
		EFFECTIVE DATE:	**9/10/10**
		PREVIOUS EFF. DATE:	**5/27/05**
[Ref.: 45 CFR Part 160 and Part 164, Subparts A and E and 42 U.S.C. §290dd-3, and implementing regulations 42 C.F.R. Part 2.]		**SUPERSEDES POL:**	**n/a**
		APPROVED DATE:	**5/27/05**

I. PURPOSE

- Ensure compliance by the CITC/IT Department Workforce with the federal HIPAA Standards, 42 U.S.C. Paragraph 290dd-3 and implementing regulations 42 C.F.R. Part 2, and related CITC policies and procedures.

II. SCOPE

This policy and all CITC - HIPAA policies and procedures of Cook Inlet Tribal Council, Inc. apply to all members of CITC's IT Workforce, including Department employees, trainees, volunteers and contractors of CITC (and applicable CITC subsidiaries) who may have access to the hard copy, verbal, and electronic protected health information of patients or clients served by CITC's covered programs and support functions.

III. DEFINITIONS

- **"Covered Programs."** Programs, services and support functions provided by a covered health care provider in connection with a transaction for which US/HHS has adopted a standard and is, therefore, subject to those US/HHS HIPAA standards by law.
- **"Covered Workforce."** Includes employees, trainees, volunteers and contractors (of CITC and applicable CITC subsidiaries) who perform work for CITC and may have access to the electronic protected health information (EPHI) of patients or clients of CITC covered programs.
- **"EPHI**." Electronic protected health information of clients/participants.
- **"HIPAA**." Health Insurance Portability and Accountability Act of 1996. (US/Health and Human Services)
- **"Hybrid Organization**." An entity that administers programs and services some of which are covered by the Health Insurance and Portability Act (HIPAA) and others that are not covered by HIPAA.
- **"IT Department."** CITC's Information and Technology Department (and Staff).
- **"PHI**." **Protected Health Information.** Protected health information means information that is created or received by CITC and relates to the past, present, or future physical or mental health or condition of a patient/client; the provision of health care to a patient/client; or the past, present, or future payment for the provision of health care to a patient/client; and that identifies the patient/client or for which there is a reasonable basis to believe the information can be used to identify the patient/client. Protected health information includes information of persons living or deceased.
- **"Support functions**." Administrative services such as billing/accounting and information technology resources.

IV. POLICY: HIPAA PRIVACY AND COMPLIANCE

A. A Hybrid Entity

Cook Inlet Tribal Council, Inc. ("CITC") is a hybrid entity with certain treatment and social service programs which are covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") while other programs and services are not similarly covered. CITC administers the following programs or departments which are known collectively as the covered programs/services and workforce by HIPAA:

- Tribal Vocational Rehabilitation (Employment and Training Department),
- Residential Treatment (Recovery Services Department, Ernie Turner Center),
- Outpatient Recovery Services (Recovery Services Department)
- Clinical Services Program (Child and Family Services Department),
- Program Evaluation (Administration)
- Billing Unit (Accounting Department), and
- Information Technology Department

No other CITC departments or programs are subject to HIPAA, or to the federal law governing the confidentiality of PHI, including alcohol and drug abuse patient records. This privacy policy is intended to cover only the Information Technology Services ("IT") department of CITC.

B. General Policy Statement on CITC/IT HIPAA Privacy and Compliance

It is CITC's policy to comply fully with the requirements of all applicable federal laws and regulations and CITC policies and procedures pertaining to the use and disclosure of HIPAA protected health information and confidentiality of substance abuse patient records in the conduct of CITC business. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict CITC's ability to use and disclose protected health information (PHI). CITC has additional duties under the federal law governing the confidentiality of alcohol and drug abuse patient records (42 U.S.C. §290dd-3, and implementing regulations 42 C.F.R. Part 2).

Members of CITC's IT workforce may have access to the individually identifiable health information of patients or clients of CITC covered programs for IT administrative control purposes only. To that end, all members of CITC's IT workforce who have access to PHI or confidential substance abuse patient records must comply with this Privacy and Compliance Policy, the more detailed Use and Disclosure Policy and Procedures *(CITC Pol. No. 2.100)*, *CITC Pol. No. 2.200 Security System (EPHI*), *CITC Pol. No. 3.300 Computer & Technology Resources Use,* and any other related CITC policy/procedure.

CITC/IT employees who perform support services for both CITC's (a) HIPAA covered programs/functions and have access to confidential substance abuse patient records and (b) non-covered programs/functions shall not use client information that they obtain in the course of providing services for the HIPAA covered components when providing services to non-covered programs. (Non-covered functions shall be treated as if they were legally separate entities from the HIPAA covered programs/functions.)

No third party rights (including but not limited to rights of CITC patient/clients, beneficiaries, business associates, or qualified service organizations) are intended to be created by this Policy. CITC's IT department reserves the right to amend or change this Policy at any time (including retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or 42 C.F.R. Part 2, the Policy shall be aspirational and shall not be binding upon CITC. This Policy addresses the requirements of HIPAA and the federal law governing the confidentiality of alcohol and drug abuse patient records, but does not address requirements under any other federal laws or state laws.

C. **CITC's Responsibilities as a HIPAA-Covered Entity**

For more specific details, see *CITC Pol. No. 2.300 Security System (EPHI)* and the related CITC procedures.

1. **Client Rights and Privacy Officer and Contact Person**

The Client Rights and Privacy Officer ("CRP Officer") for CITC is appointed by the President/CEO. The Officer is responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and CITC's more detailed Use and Disclosure Policy and Procedures (CITC Pol. No. 2.100). The CRP Officer will also serve as the contact person for patient/clients who have questions, concerns, or complaints about the privacy of their PHI:

Corporate Client Rights and Privacy Officer
Cook Inlet Tribal Council, Inc.
3600 San Jeronimo
Anchorage, AK 99508
(907) 793-3600

2. **Covered Program HIPAA Policy Liaison.**

Each HIPAA-covered program/unit shall have a named HIPAA Policy Liaison who is responsible for ensuring that the program (a) complies with the HIPAA Security Policy, (b) implements the HIPAA Security Policy within the program unit, (c) maintains the confidentiality of all EPHI created or received by the program unit from the date such information is created or received until it is destroyed, (d) trains all Workforce members of the program unit about CITC's HIPAA Security Policy, and (e) contacts the Corporate Compliance Officer for advising in Security Policy-related problem resolution.

3. **Workforce Training**

It is CITC's policy to train all employees who have access to PHI regarding its privacy policies and procedures. The CRP Officer is charged with developing training schedules and programs so that all covered workforce members receive the training necessary and appropriate to permit them to carry out their functions within CITC's covered programs.

4. **Technical, Physical and Administrative Safeguards and Firewall**

CITC's IT Department has established appropriate technical, physical and administrative safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. These safeguards are more fully described in the security policies and procedures of the IT Department and *CITC Pol. No. 2.300 Security System (EPHI).*

CITC Information Technology has instituted the safeguards to limit unnecessary and inappropriate access to the protected health information and confidential substance abuse records maintained by the IT Department. In every case, the CITC IT workforce will ensure that protections of privacy and confidentiality applied to the general public in order to prevent the disclosure of PHI or confidential substance abuse records during office visits would be applied to non-covered program personnel, unless a HIPAA and 42 CFR Part 2 compliant authorization is in place.

5. **Privacy Notice**

The CITC Client Rights and Privacy Officer is responsible for developing and maintaining a Notice of Privacy Practices that describes:

- The uses and disclosures of PHI that may be made by CITC;
- The individual's rights; and
- CITC's legal duties with respect to the PHI.

6. **Complaints**

a. **Internal Submission of a Complaint.** The CRP Officer will be CITC's contact person for receiving complaints. The CRP Officer is responsible for creating a process for individuals to lodge complaints about CITC's privacy procedures and for creating a system for handling such complaints. *CITC Pol. No. 3.100 Client Rights and Grievance* provides the steps for complaint resolution.

b. **External Submission of a Complaint**. An individual also may file a complaint with the Secretary of the U.S. Department of Health and Human Services ("DHHS").

7. **Sanctions for Violations of Privacy Policy**

All members of CITC's IT workforce with access to PHI must comply with this Policy and with CITC's *Pol. No. 2.100 Use and Disclosure*, and *Pol. No. 2.300 Security System (EPHI)*, and any other related CITC policy and procedure. Sanctions for using or disclosing PHI in violation of this Policy will be imposed in accordance with CITC's policies regarding employee discipline. The severity of the sanction will depend on the facts and circumstances of the violation and may include discipline up to and including immediate termination.

8. **Mitigation of Inadvertent Disclosures of Protected Health Information**

CITC shall mitigate, to the extent reasonable and feasible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. An IT workforce member who becomes aware of a disclosure of protected health information (either by an employee of CITC or an outside business associate, qualified service organization, consultant, or contractor) that is not in compliance with this Policy must immediately report the disclosure to the CRP Officer. The CRP Officer will determine the reasonable and appropriate steps, which may mitigate the harm to the patient/client. The method of mitigation will depend on the facts and circumstances of the unauthorized use or disclosure as determined in the discretion of the Privacy Officer. After conducting a thorough investigation of the incident the CRP Officer will work with the affected department to document the incident and implement appropriate protective measures.

9. **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy**

Neither CITC nor any of its workforce members acting within the course and scope of employment shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, or eligibility under CITC's covered programs.

10. **Documentation**

CITC/IT Department privacy policies and procedures shall be documented and maintained for at least six (6) years. Policies and procedures will be amended as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures will be documented and become effective only with respect to PHI created or received after the effective date of the amended policies and procedures.

CITC IT Department shall create, maintain and store log files and tracking information for evidentiary purposes in the event there is a dispute against CITC or to a court-ordered subpoena for specified PHI information that is stored regarding a client. Such action taken by the CITC IT Department in response to such a request shall be documented and maintained in a confidential file status.

V. POLICIES ON USE AND DISCLOSURE OF PHI AND CONFIDENTIAL SUBSTANCE ABUSE RECORDS

A. **General**

CITC will use and disclose PHI only as permitted under HIPAA and 42 C.F.R. Part 2. CITC ~~i~~s not responsible for voluntary disclosures of PHI by the individual to whom the information pertains.

B. **Access to PHI is Limited to Certain IT Department Employees**

The use and disclosure of protected health information shall be limited to the minimum necessary extent to perform a particular CITC function. Access to protected health information by the CITC/IT Department workforce is limited to a job-related need for access in order to administer the network functions only. The protected information the CITC/IT workforce accesses and maintains in the course of performing such network administration duties may include treatment, payment, eligibility and follow up information, which may only be used or disclosed in accordance with this Policy and CITC's more detailed Use and Disclosure Procedures. The protected information will be secured with reasonable technical, physical and administrative protections to prevent unauthorized use and disclosure.

C. **Permitted Uses and Disclosures: Treatment, Payment and CITC Operations**

During the course of conducting routine network administration duties, IT personnel may occasionally and inadvertently encounter PHI; however, in all instances, IT personnel are not responsible for, nor authorized to provide any PHI information to anyone. IT personnel are bound by CITC policies and procedures to maintain confidentiality.

Treatment. Treatment includes the provision of health care. IT workforce members are not involved in direct treatment services within the course and scope of their employment with CITC. However, IT workforce members may encounter, access or maintain PHI or confidential substance abuse information regarding treatment in the course of performing their network administration duties.

Payment. Payment includes activities undertaken to obtain reimbursement for health care services provided by CITC. IT workforce members are not involved in obtaining payment for CITC services within the course and scope of their employment. However, IT workforce members may encounter, access or maintain PHI or confidential substance abuse information regarding payment in the course of performing their network administration duties.

Operations. PHI may be disclosed for purposes of CITC IT's operations. For CITC substance abuse programs, no written patient authorization is required for communication within IT or between IT and another CITC entity having direct administrative control over IT or the covered program providing patient substance abuse services. CITC IT operations may include the maintenance of databases for quality assurance activities of other covered programs, internal and external data collection and inputting regarding covered programs and other operations as necessary to maintain and improve the computer network. IT workforce members may encounter, access or maintain PHI or confidential substance abuse information regarding CITC covered programs' operations in the course of performing their network administration duties.

D. **No Disclosure of PHI for Non-CITC Purposes**

PHI may not be used or disclosed that pertain to the operations of CITC's non-covered programs unless the patient/client has provided an authorization for such use or disclosure (discussed further in CITC's Use and Disclosure Procedures) or such use or disclosure is required by applicable state or federal law and particular requirements under HIPAA are met. See CITC's Use and Disclosure Procedures for more detail on required and permitted disclosures.

E. **The Minimum-Necessary Standard**

When PHI is used or disclosed by CITC, the amount disclosed or used generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

VI. POLICIES ON INDIVIDUAL RIGHTS – HIPAA provides patients with individual rights that shall be recognized and enforced by CITC. The CITC CRP Officer shall develop procedures describing these rights and how to recognize these rights.

CITC HIPAA Policies and Procedures

Pol. No. 1.030	Subpoenas, Court Orders, and Warrants Policy
Pol. No. 2.100	HIPAA Use and Disclosure
Pol. No. 2.200	HIPAA Privacy and Compliance
Pol. No. 2.300	HIPAA Security System (EPHI)
Pol. No. 3.100	Client Rights and Grievance Policy
Pol. No. 3.300	Computer and Technology Resources Policy

Forms:

HIPAA Acknowledgement Notice of Privacy Practices
HIPAA Notice of Privacy Practices
Authorization for Release of PHI