WTCSB HIPAA SANCTIONS POLICY

PURPOSE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with Privacy Policies and Procedures of the entity, or the requirements of the Rule (45 CFR SS 164.530(e)(1). Accordingly, it is the intention of the Western Tidewater Community Services Board (WTCSB) to ensure the confidentiality and integrity of consumer and/or employee protected health information (PHI) as required by law, professional ethics, and accreditation and/or licensure requirements. This policy establishes agency policy, guidance, and standards for workforce performance expectations in carrying out the provisions of HIPAA, and the corrective action(s) that may be imposed to address privacy violations.

POLICY

Consumer and/or employee PHI information will be regarded as confidential, and may not be used or disclosed except to authorized users for approved purposes. Access to PHI is only permitted for direct consumer care, approved administrative and/or supervisory functions, or with approval of the Privacy Officer (Quality Assurance Director), Executive Director, or Human Resources Director.

Permitted Use and Disclosures

The WTCSB is permitted to use or disclose PHI in the following instances:

- To the individual who is the subject of the PHI;
- In compliance with consent to carry out treatment, payment or health care operations;
- Without consent, if consent is not required and has not been sought;
- In compliance with valid authorization;
- Pursuant to an Agreement.

Required Disclosures

The WTCSB is required to disclose PHI in the following instances:

- To an individual, when requested under and as required by SS164.524 (Access of individuals to PHI) or SS164.528 (Accounting of disclosure of PHI) of the HIPAA Regulations;
- To specific private entities that provide services under contractual agreements (health benefits, life insurance, Workers Compensation, etc.) in order to provide such services;
- When required by the Privacy Officer, Executive Director, or Human Resources Director to investigate or determine compliance with HIPAA requirements.

Minimum Necessary

When using or disclosing PHI, or when requesting PHI from another covered entity, the WTCSB will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

Sanction Exemptions

Sanctions will not apply to disclosures by employees who are ***whistleblowers*** or ***crime victims***. The WTCSB is not considered to have violated PHI disclosure requirements if the disclosure is by an employee or business associate as follows:

Disclosure by Whistleblowers:

- The employee is acting in good faith on the belief that the WTCSB has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or,

- That the care, services and conditions provided by the WTCSB potentially endangers one (or more) WTCSB consumers, employees or a member of the general public; or,

- The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered entity; or,

- The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the WTCSB; or

- The disclosure is made to an attorney retained by or on behalf of the employee or business associate for the purpose of determining legal options regarding disclosure conduct.

Disclosure by Crime Victims:

A covered entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official about the suspected perpetrator of the criminal act, and the disclosed PHI is limited to identification and location purposes.

Mitigation

Mitigating circumstances include conditions that would support reducing the sanction in the interest of fairness and objectivity. The WTCSB will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of PHI in violation of HIPAA regulations.

Retaliation

The WTCSB will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

- Exercises his rights or participates in the WTCSB complaint process; or,
- Files a complaint with the Secretary of Health and Human Services; or,
- Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing; or,
- Opposes any act or practice unlawful under HIPAA, providing that the individual acted in good faith, believing that the practice was unlawful, the manner of opposition is reasonable, and does not involve disclosure of PHI in violation of HIPPA regulations

PROCEDURES

DISCIPLINARY SANCTIONS

Employees found to have violated PHI disclosure provisions will be disciplined in accordance with WTCSB Policy #6.1, *Standards of Conduct*, up to and including termination of employment. The type of sanction will depend on the intent of the individual and severity of the violation. The offenses listed below, while not all inclusive, are organized according to the severity of the violation.

Group I: ***Improper and/or unintentional disclosure of PHI or records***.
This level of breach occurs when an employee unintentionally or carelessly accesses, reviews or reveals consumer or employee PHI to himself or others without a legitimate need-to-know. Examples include, but are not limited to: employees who discuss consumer information in a public area; an employee leaves a copy of consumer medical information in a public area; an employee leaves a computer unattended in an accessible area with consumer information unsecured.

Group II: Unauthorized use and/or misuse of PHI or records.
This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with WTCSB policies and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee looks up birth dates, address of friends or relatives; an employee accesses and reviews the record of a consumer out of curiosity or concern; an employee reviews a public personality's record.

Group III: Willful and/or intentional disclosure of PHI or records.
This level of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent. Examples include, but are not limited to: an employee reviews a consumer record to use information in a personal relationship; an employee compiles a mailing list for personal use or to be sold.

DOCUMENTATION

Initial Reporting

Employees who observe or are aware of a breach must immediately report it to his/her Supervisor. The Supervisor will report the breach to the Privacy Officer, who will notify the Executive Director and Human Resources Director.

Failure to report a breach of which one has knowledge will result in appropriate disciplinary action. Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

Clear-cut Level I Breaches

For a breach involving any staff that is clearly a Level I breach, the Privacy Officer, in conjunction with the employee Supervisor, Executive Director and Human Resources Director, will develop and implement an appropriate Plan of Correction, and in a timely manner.

Breaches Other Than Clear-cut Level I Breaches

For all levels other than a clear-cut Level I breach, the Privacy Officer will establish an Investigation Team that will include senior Management and Human Resources representation, and legal counsel participation or consultation.

The Investigation Team will conduct an appropriate investigation, commensurate with the level of breach and specific facts. This may include, but is not limited to, interviewing the employee accused of the breach, interviewing other employees or consumers, and reviewing documentation.

Upon conclusion of the investigation, the Investigation Team will prepare a written report including all findings and conclusions regarding the alleged breach, and forward it to the Privacy Officer. The Executive Director will make final determination of the appropriate disciplinary action, based on the report of the Investigation Team.

Reporting and Filing Requirements

For all levels of breach, after final resolution the initial report and all supporting documentation will be filed in a confidential file with the Privacy Officer. A copy of the report and supporting documentation will also be placed in the Personnel File of the employee.