

SUBJECT: HIPAA SANCTIONS

EFFECTIVE
DATE: 04-30-10 (replaces 05-19-04)

APPROVED BY:

Reviewed (no changes): 03-31-11 _____

Executive Director

POLICY

The Health Insurance Portability and Accountability Act of 1996 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 14.530(e)(1)). Accordingly, it is the intention of McIntosh Trail Community Service Board 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. 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, Executive Director or Employee Relations Director.

Sanction Exemptions

- A. Sanctions do not apply to whistleblowers, provided that
- a. The workforce member making a disclosure of protected health information (PHI) believes that:
 1. The care, services, or conditions provided by the organization potentially endanger one or more individuals, workers, or the public OR
 2. The workforce member or business associate believes, in good faith, that the organization has engaged in conduct that is unlawful or otherwise violates professional or clinical standards.
- AND
- b. The disclosure of PHI made by the workforce member is to:
 1. An appropriate oversight agency, including but not limited to the Long Term Care Ombudsman program, or a public health authority,
 2. An appropriate healthcare accreditation organization, or
 3. An attorney for the purposes of determining the legal options with regard to the conduct of the workforce member or business associate.
- B. Disclosure by Crime Victims:
Sanctions do not apply to workforce members who are victims of a criminal act and disclose protected health information (PHI) to a law enforcement official. The disclosed PHI must be about a suspected perpetrator of the criminal act and is limited to the following information:
- a. Name and address;
 - b. Date and time of treatment.

SUBJECT: HIPAA SANCTIONS

EFFECTIVE
DATE: 04-30-10 (replaces 05-19-04)

APPROVED BY:

Reviewed (no changes): 03-31-11 _____

Executive Director

POLICY (Continued)

Mitigation

Mitigating circumstances include conditions that would support reducing the sanction in the interest of fairness and objectivity. McIntosh Trail CSB 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

McIntosh Trail CSB will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

- Exercises his rights or participates in the organization's 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 disclosures of PHI in violation of HIPAA regulations.

PROCEDURES

Employees found to have violated PHI disclosure provisions will be disciplined in accordance with McIntosh Trail Community Service Board policies, 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.

1. 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.
2. 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 McIntosh Trail CSB policies and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee looks up birth dates, addresses 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.

SUBJECT: HIPAA SANCTIONS

EFFECTIVE
DATE: 04-30-10 (replaces 05-19-04)

APPROVED BY:

Reviewed (no changes): 03-31-11 _____

Executive Director

PROCEDURES (Continued)

3. 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 Employee Relations 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 Employee Relations 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 Employee Relations 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.

SUBJECT: HIPAA SANCTIONS

EFFECTIVE
DATE: 04-30-10 (replacing 05-19-04)

APPROVED BY:

Reviewed (no changes): 03-31-11 _____

Executive Director

PROCEDURES (Continued)

HIPAA Sanctions

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Through subtitle F of title H of that law, the Congress added to title XI of the Social Security Act a new part C entitled "Administrative Simplification." (Public Law 104-191) affects several titles in the United States Code. Hereafter, the Social Security Act is referred to as the Act.

Section 1176 of the Act establishes a civil monetary penalty for violations of the provisions in Part C of title XI of the Act, subject to several limitations. Penalties may not be more than \$100 per person per violation and not more than \$25,000 per person for violations of a single standard for a calendar year. The procedural provisions in section 1128A of the Act "Civil Monetary Penalties," are applicable.

Section 1177 of the Act establishes penalties for knowing misuse of unique health identifiers and individually identifiable health information: (1) A fine of not more than \$50,000 and/or imprisonment of not more than 1 year; (2) if misuse is "under false pretenses", a fine of not more than \$100,000 and/or imprisonment of not more than 5 years; and (3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000 and/or imprisonment of not more than 10 years. Note that these penalties do not affect any other penalties, which may be imposed by other Federal programs, including ERISA.

In addition to the penalties prescribed by law, violations of the agency's Privacy Policies and Procedures may result in corrective action to include informal counseling, additional training or other measures to address the violation, and in appropriate cases, disciplinary action may be imposed, up to and including dismissal from employment. Employment sanctions will take into account all circumstances associated with the violation, including whether there is a pattern of similar violations, the extent of the violator's training, skills, and experience, and the potential or actual harm done. Sanctions will be consistent with the provisions of the McIntosh Trail Disciplinary Personnel Policies/State Personnel Board Rules.