Employee Sanction Policy

__________________________________(Practice Name)

PURPOSE:

As required by HIPAA, this policy sets forth the appropriate sanctions for workforce members who fail to comply with the privacy and security policies and procedures set by ___________________(Practice Name).

Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with security and privacy policies and procedures to deter noncompliance. Having a policy and procedures for employees reinforces the commitment that ___________________(practice name) have to safeguard Protected Health Information and confidential information and provides:

1. A clear and consistent response to a violation;
2. A consistent corrective disciplinary action for the same type of offense;
3. Good employee compliance with security and privacy safeguards designed to protect PHI;
4. A rapid response in applying sanctions which sends a message of the commitment to protect patient privacy as well as decreasing the risk to the organization of violating HIPAA;
5. Strengthens the organization’s position for dispute resolution;
6. Decreases the organization’s vulnerabilities to civil actions and lawsuits;
7. May affect how the Office of Civil Rights and the federal judiciary sanction the organization;
8. Decreases further state and federal intervention.

DEFINITIONS:

Workforce: Employees of ________________(practice name) and any independent contractors contracted to perform duties for and by (practice name)

Confidential/Sensitive Information:
Includes, but is not limited to, PHI of patients, including electronic PHI, any information about other employees, any computer log-on codes or passwords, personal physician information, any financial information about (practice name),

Protected Health Information:
(PHI); Any identifiable demographic information and other information which relates to an individual’s past, present or future physical or mental health or condition for which there is a reasonable cause to believe it can be used to identify that individual. Genetic information is now considered to be health information. PHI applies to communication in written, verbal or electronic form used in records, social media, internet, intranet, etc.
Sanction Guidance Table:
A table that sets out examples of potential violations that adjusts the
disciplinary action based on the severity of the violation.

POLICY:
Any report or knowledge of a HIPAA privacy or security breach shall be investigated; a risk analysis
performed and any mitigation performed. The workforce member(s) involved in the breach shall be
disciplined according to the extent and intent of the breach. Refer to Attachment A Sanction Guidelines
Table.

The Sanction Guidelines Table shall be used to help determine the level of severity of the violation and
the appropriate employee sanction associated with the severity level.

Procedures:
1. Any HIPAA breach or suspected breach shall be reported to the Privacy and/or Security Officer.
   A. Examples of an actual breach include, but are not limited to:
      • Emailing, faxing, mailing PHI to the wrong recipient.
      • Emailing, faxing, mailing information that contains PHI to the correct recipient, but not
de-identifying it first, if applicable.
      • Use/disclosure of confidential/sensitive information.
      • Loss or theft of media in electronic form or paper that contains PHI and/or
        confidential/sensitive information.
   B. Examples of a suspected breach include, but are not limited to:
      • Seeing an employee, with no ‘need to know’ rights, reading files with PHI.
      • Leaving information with PHI open on an unattended computer.
      • Leaving files on desk overnight and not in a secure location.

2. Any unauthorized sensitive information sharing, stealing or copying needs to be reported to the
   Privacy and/or Security Officer.
   A. Examples of sensitive information sharing include, but are not limited to:
      • An employee taking a file from the office to show a friend or family member.
      • An employee seen writing down bank account numbers or other PHI for personal use.
      • An employee taking a file out of the office without permission from the Privacy or
        Security Officer.

Determining a Breach
1. The Privacy Officer and Security Officer will determine if a HIPAA breach or sensitive information
   breach has occurred.
2. If a HIPAA breach has occurred it shall be determined if the breach needs to be reported to the
   Department of Health and Human Services.
3. It is the responsibility of X to make a recommendation to X based on the findings of the risk
   analysis and use of the sanction chart as a guideline.
Records

1. Breach investigation notes and sanction documentation will be kept by the Privacy Officer for six (6) years.
2. A copy of the workforce member’s sanction shall be retained in the workforce member’s personnel file.
3. This policy shall be retained for six (6) years from its effective date.