SANCTION POLICY

Purpose

To ensure appropriate sanctions will be applied to workforce members who violate the requirements of HIPAA, Practice's security policies, Directives, and/or any other state or federal regulatory requirements.

Policy

It is the policy of the Practice that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Practice will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The Practice will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Practice's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Definitions

Workforce Member

Employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive Information

Includes, but not limited to, the following:

- *Protected Health Information (PHI)* – Individually identifiable health information in any form or media, whether electronic, paper, or oral.
- *Electronic Protected Health Information (ePHI)* – PHI that is in electronic format.
- *Personnel files* – Any information related to the hiring or employment of any individual who is or was employed by the Practice.
- *Payroll data* – Any information related to the compensation of an individual during employment with the Practice.
- *Financial/accounting records* – Any records related to accounting practices or financial statements of the Practice.
- *Other information that is confidential* – Any other information sensitive in nature or considered to be confidential.

Availability

Refers to data or information being accessible and useable upon demand by an authorized person.

Confidentiality

Refers to data or information NOT being made available or disclosed to unauthorized persons or processes.

Integrity

Refers to data or information that has NOT been altered or destroyed in an unauthorized manner.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information you do not need to know to do your job • Sharing computer access codes (user name or password) • Leaving computer unattended while being able to access sensitive information • Disclosing sensitive information with unauthorized persons • Copying sensitive information without authorization • Changing sensitive information without authorization • Discussing sensitive information in a public area or in an area where the public could overhear the conversation • Discussing sensitive information with an unauthorized person • Failing or refusing to cooperate with the Privacy Officer or authorized designee

Level	Description of Violation
2	• Second occurrence of any Level 1 offense (does not have to be the same offense) • Unauthorized use or disclosure of sensitive information • Using another person's computer access code (user name or password) • Failing or refusing to comply with a remediation resolution or recommendation
3	• Third occurrence of any Level 1 offense (does not have to be the same offense) • Second occurrence of any Level 2 offense (does not have to be the same offense) • Obtaining sensitive information under false pretenses • Using or disclosing sensitive information for commercial advantage, personal gain, or malicious harm

Recommended Disciplinary Actions

In the event a workforce member violates the Practice's privacy and security policies or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand; or suspension • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
3*	• Termination of employment or contract • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

* Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Practice.

References

U.S. Department of Health and Human Services

Health Information Privacy. Retrieved April 24, 2009, from http://www.hhs.gov/ocr/privacy/index.html

Related Policies

Information Security Policy

Acknowledgment

I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for

_____ (practice name).

Workforce Member Signature: _____ Date: _____