**POLICY & PROCEDURES**

***Defining the Overall Approach toward Meeting a Requirement***

### **Sanction Policy §164.308(a)(1)(ii)(C)**

### **Effective Date:** <Month Day, Year>

### **Policy Number:** <If applicable> **Rev.** 0

**Policy:** We must comply with all of our HIPAA security policies and procedures or disciplinary action will be taken. Disciplinary action is dependent upon many variables and will at a minimum, take into account the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of PHI on a case-by-case basis. All employees must report suspected or known workforce members who are non-compliant with our policies and procedures to the Security Official.

**Procedures:** The sanction policy applies to our entire workforce. Sanctions are commensurate with the severity of non-compliance with our security policies and procedures. We provide regular security training and awareness for our workforce members to help prevent any non-compliance of our security policies and procedures. Our organization will not intimidate or retaliate against any individual who report acts or practices that are unlawful, provided the individual in good faith believes that the practice is unlawful and reporting such a case is reasonable and does not disclose PHI in violation with HIPAA law.

**Details:** The sanction procedures include but are not limited to the following disciplinary actions:

Level 1 - Accidental Breach:

Possible Scenarios:

* Employee does not log off the computer after use.
* Employee leaves computer logged-in an unattended without locking the computer screen in an unsecure area.
* Employee leaves PHI document unattended and face up in an unsecure area.
* Employee faxes the wrong PHI to another practice.
* Employee forgets to get a signed acknowledgment of receipt of the Notice of Privacy Practices.
* Employee emails PHI to the wrong email address.

Sanction:

* Verbal warning and re-education
* Continued offenses lead to progressive discipline up to and including termination.

Level 2 - Intentional Breach without Harmful or Dishonest Intentions:

Possible Scenarios:

* Viewing patient records out of curiosity.
* Sharing PHI because the information is interesting (not for treatment purposes).
* Employee shares computer password.
* Discussion of patient information in an unsecured area.

Sanction:

* Written warning and re-education
* Continued offenses lead to progressive discipline up to and including suspension or termination.

Level 3 - Willful or Intentional Breach with Harmful or Dishonest Intentions:

Possible Scenarios:

* Using PHI for personal gain (marketing without authorization).
* Using PHI to cause harm (exposing information to unauthorized individuals because of dislike for the owner of the PHI).
* Gives access to a restricted area to an unauthorized individual.
* Gives access to PHI to an unauthorized individual.

Sanction:

* Written termination and possible legal action.

**Location of supporting documentation:** If so, identify the document and location it is stored here.

## REVISION HISTORY

| Revision | Date | Initiator | Nature of Change |
| --- | --- | --- | --- |
| 0 |  |  | Initial draft |
| 1 |  |  |  |