Policy: Sanctions will be imposed on individuals who violate privacy and information security policies and procedures. The work force will be reminded at least annually through our work force awareness program of the potential consequences.

Sanctions may include:
- Oral or written warnings
- Immediate termination of employment, of work agreement with students/trainees and volunteers, and/or of business contract, as appropriate
- External reporting, possibly resulting in civil and criminal legal consequences:
  - To government agencies, such as the Secretary of Health and Human Services
  - To law enforcement
  - To licensing and registration boards

Purpose: This organization is committed to ensuring the privacy and security of information under our protection. We intend these sanctions to serve as a deterrent to violations. Under regulations such as HIPAA privacy and security rules, we are obligated to enforce our privacy and security policies and procedures. Therefore, when such policies and procedures are violated, we will respond by mitigating breaches and sanctioning those responsible.

Scope: This policy applies to our full work force. It covers all privacy and information security policies, standards, rules, and procedures. Further, it applies even when an instance is not explicitly prohibited, but when it is clearly counter to the intent of the body of policies, procedures, etc.

General rules:
1. Reporting
   Workforce members and Business Associates must report actual and suspected violations and breaches. Failure to report a breach of which one has knowledge may result in disciplinary action. Falsely reporting a breach in bad faith or for malicious reasons will result in disciplinary action.
2. **Sanctions**
   Workforce sanctions will be based on:
   - The severity of the violation and its impact
   - Whether the violation was intentional and, if so, what the intent was
   - Whether the violation is part of a pattern of improper behavior regarding privacy and security

   Mitigating factors will be considered.

3. **Sanction Review**
   Before it is imposed, a proposed sanction will be reviewed by the Compliance Officer to ensure appropriateness, consistency, and fairness across all members of the workforce.

4. **Documentation**
   Each case will be documented and filed in the workforce member’s record, where it will be retained for a minimum of six years. Documentation must include:
   - Date of incident
   - Report submitted by
   - Date submitted
   - Investigated by
   - Name of employee(s) involved
   - Name of client(s) involved
   - Type of incident/Complaint
   - Source of initial report of incident/Complaint
   - Action taken
   - Brief description of incident
   - Results of investigation
   - Conclusions

5. **Incident Analysis and Mitigation**
   During and following this process, the organization will analyze the consequences of the breach or violation and consider whether mitigation measures must be taken to protect a patient, a staff member, the organization, etc. This process is part of this organization’s privacy and security incident response plan.

6. **Exceptions**
   Work force members are not considered to have violated HIPAA if the disclosure of PHI is as follows.

   **Whistleblowers:** Sanctions will not apply to disclosures by work force members acting in good faith:
• In the belief that this organization has engaged in conduct that is unlawful or otherwise violates professional or clinical standards;
• Or that care or services provided by this organization potentially endanger patients, employees, or members of the 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 healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by this organization;
• Or the disclosure is made to an attorney retained by or on behalf of the work force member or Business Associate for the purpose of determining legal options regarding disclosure conduct.

Crime victims: A Covered Entity is not considered to have violated HIPAA’s PHI use and disclosure requirements if a member of its work force 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.

7. Non-Retaliation
   This organization will not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against an individual who:

   • Exercises his rights or participates in this organization’s complaint process;
   • Files a complaint with the Secretary of Health and Human Services, Office for Civil Rights (OCR), or Centers for Medicare and Medicaid Services (CMS);
   • Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing;
   • 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 HIPAA regulations.