**Integrity Controls Policy**

**PURPOSE:**

[Insert Covered Entity or Business Associate name], which handles ePHI, will implement the ability to authenticate, which is the process used to validate data integrity, to verify that the data sent is protected against unauthorized alteration or destruction during transmission over electronic communications networks.

**DEFINITIONS:**

1. Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.
2. Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form.
3. Electronic Protected Health Information (ePHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
4. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors 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.

**POLICY:**

1. The Security Officer will approve the electronic mechanisms that will be implemented to protect ePHI from unauthorized alteration or destruction and to authenticate the integrity of ePHI during transmission.
2. The Security Officer will determine the appropriate steps to confirm effective implementation of the integrity controls, to review and update them as necessary as defined by the Evaluation policy.
3. The Security Officer will provide affected workforce members with training and awareness regarding integrity controls implemented to protect ePHI from unauthorized alteration or destruction during transmission over electronic communications networks.
4. The Security Official will ensure that actual and potential damage to the integrity of confidential or sensitive information, including ePHI, is appropriately addressed.
5. Transmitting ePHI via a removable media such as a flash drive or removable hard drive requires the files to be password protected.
   1. The receiving entity shall be authenticated before transmission.
6. IT shall maintain adequate firewall protection of the network.
   1. The firewall shall be configured to “deny” rather than “allow” as the default setting.
   2. Unused firewall ports shall be closed.
   3. IT staff shall examine firewall logs and reevaluate the security configurations periodically (Insert time period/every week, every month, etc.).
7. All encryption mechanisms utilized for transmission of ePHI will support a minimum of 128 bit encryption.

**VIOLATIONS:**

Any known violations of this policy should be reported to the Security Officer.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with [Insert Covered Entity or Business Associate name] procedures.

[Insert Covered Entity or Business Associate name] may advise law enforcement agencies when a criminal offense may have been committed.