HIPAA Compliance Policy

Best S.T.E.P. Forward has adopted this General HIPAA Compliance Policy to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the HITECH Act of 2009 (ARRA Title XIII). We acknowledge our responsibility to protect individually identifiable health information under HIPAA regulations, other federal and state laws, and general professional ethics. All personnel of Best S.T.E.P. Forward must comply with this policy. Demonstrated competence in this policy is crucial for every member of the workplace. Employees who violate this policy are subject to disciplinary action, up to and including termination.

Definitions

- **Protected Health Information (PHI):** Any individually identifiable health information held by a covered entity, including any part of a patient's medical record or payment history.
- **Covered Entity:** Any organization that transmits health information in electronic form in connection with a HIPAA transaction.

1. Compliance Overview

- All employees must understand HIPAA regulations, including the Privacy Rule, Security Rule, and Breach Notification Rule.
- Regular training will be provided to ensure ongoing awareness and understanding of HIPAA requirements.
- **Access Restrictions:** If you are not on staff, you are prohibited from accessing or viewing client information, including any portals used to schedule clients.

2. Privacy Policy

- **Use and Disclosure of PHI:** PHI may only be used and disclosed for treatment, payment, and healthcare operations, or as permitted by law.
- **Patient Rights:** Patients have the right to access their PHI, request amendments, receive an accounting of disclosures, and request restrictions on certain disclosures.

3. Security Policy

- **Administrative Safeguards:** Access to PHI will be limited to authorized personnel only. A designated HIPAA Privacy Officer will oversee compliance.
- **Physical Safeguards:** PHI stored in physical format must be kept in locked areas. Electronic devices containing PHI must be secured.

- **Technical Safeguards:** Use of encryption and secure passwords is required for electronic PHI. Regular audits will be conducted to ensure compliance with security protocols.

4. Incident Response

- **Reporting Breaches:** All employees must report suspected breaches of PHI to the HIPAA Privacy Officer immediately.
- **Investigation:** All reported incidents will be investigated promptly, and appropriate actions will be taken to mitigate any harm.

5. Enforcement and Discipline

- **Compliance Monitoring:** Compliance with this policy will be monitored regularly. Violations may result in disciplinary action, up to and including termination.

6. Policy Review and Updates

This policy will be reviewed annually and updated as necessary to ensure ongoing compliance with HIPAA regulations.