Attachment E: Guide to Acceptable Information Privacy and Security Practices

Written for:
West Virginia Public Employees Insurance Agency's (PEIA) Approved Weight Management Sites

## Section 1: Purpose of This Guide

The PEIA is committed to protecting its members' personal information. Further, the PEIA is required by federal law to implement policies and procedures that clearly reflect this commitment. As the PEIA weight management program expands to facilities which aren't traditionally health care providers (fitness centers, etc.) and therefore may not be covered under these same laws, it desires to ensure that these facilities have comparable practices in place which also protect our members. This document is designed to inform the PEIA-approved weight management facilities of what the PEIA expects with regard to information privacy and security. If the PEIA finds that a facility's practices aren't consistent with any of the requirements herein, it reserves the right to remove the facility from the list of approved sites. **By billing for these services you are agreeing to comply with each of the provisions listed in section 2.**

## Section 2: PEIA's Privacy and Security Expectations

Since some sites are not traditional health care providers and may not be aware of the many responsibilities surrounding HIPAA, PEIA will provide you with some language which summarizes a provider's responsibility under HIPAA. This language was excerpted from an agreement which is typically signed by organizations performing a function on PEIA's behalf. PEIA expects all of its providers, at a minimum, to have policies and procedures in place consistent with this language. This language should only be used as a guide and by no means is all-inclusive of the requirements.

Further, since you will be billing Wells Fargo for these services, you are agreeing to accept the PEIA fee schedule and are bound by the applicable requirements of WV Code §5-16-1 et seq.

1. **Definitions**.

A reference to "Associate" or "Business Associate" refers to your facility.

a. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

b. **Privacy Rule**. Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E, as amended.

c. **Security Rule**. Security Rule means the standards for the security of electronic protected health information found at 45 CFR Part 164, subpart C, as amended.

d. **Required by Law**. Required by Law shall have the meaning set forth in 45 CFR 164.103.

2. **PHI Disclosed; Permitted Uses**.

a. **PHI Described**. PHI (as defined in 45 CFR 160.103) disclosed by the Covered Entity to the Business Associate, PHI created by the Business Associate on behalf of the Covered Entity, and PHI received by the Associate from a third party on behalf of the Covered Entity are disclosable under this Agreement. The disclosable PHI is limited to the minimum necessary to complete the tasks, or to provide the services, associated with the terms of the Agreement.

b. **Purposes**. Except as otherwise limited in this Agreement, Associate may use or disclose the PHI on behalf of, or to provide services to, the Covered Entity for

the purposes necessary to complete the tasks associated with, and required by the terms of the Agreement, if such use or disclosure of the PHI would not violate the Privacy or Security Rules if done by Covered Entity or violate state law or violate the minimum necessary policies and procedures of the Covered Entity.

3. **Obligations of Business Associate**.

a. **Stated Purposes Only**. The PHI may not be used by the Associate for any purpose other than stated in this Agreement or as required or permitted by law.

b. **Limited Disclosure**. The PHI is confidential and will not be disclosed by the Associate other than as stated in this Agreement or as required or permitted by law.

c. **Safeguards**. The Associate will use appropriate safeguards to prevent use or disclosure of the PHI except as provided for in this Agreement, as stated in 164.504(e)(2)(ii)(B). Associate shall maintain an appropriate level of administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI it creates, receives, maintains or transmits on behalf of Covered Entity in accordance with, at a minimum, the Security Rule. This shall include, but not be limited to:

(i.) Limitation of the groups of its employees or agents to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Agreement, and the use and disclosure of the minimum PHI necessary. For example, a limited number of employees should have access to the on-line system used to administer the program and refrain from sharing passwords used to access the system;

(ii.) Appropriate notification and training of its employees or agents to whom the PHI will be disclosed in order to protect the PHI from unauthorized disclosure;

(iii.) Maintenance of a comprehensive written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations.

d. **Compliance With Law**. The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws to which Associate is subject relating to confidentiality of PHI, as a business associate of Covered Entity.

e. **Report of Disclosure and Security Incident**. The Associate will promptly report to the Covered Entity, in writing, any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware. Moreover, the Associate agrees to promptly report to the covered entity any "security incident," as defined by 45 CFR §164.304, as amended, of which it becomes aware.

f. **Mitigation**. Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Agreement.

g. **Documentation**. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §§164.528 and 164.316. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include: (i) the date of disclosure; (ii) the name of the entity or person who received the PHI, and if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of purposes of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

h. **Accounting Rights**. Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Covered Entity the PHI required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under 45 CFR § 164.528.

i. **Access to PHI**. Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR § 164.524.

j. **Amendment of PHI**. Within ten (10) days of receipt of a request from Covered Entity for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526.

k. **Retention of PHI**. Notwithstanding section 4.a. of this Agreement, Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the PHI required under Section 3.g. of this Agreement for a period of six (6) years after termination of the Agreement, or longer if required of Associate under state law.

l. **Agents, Subcontractors Compliance**. The Associate will ensure that any of its agents, including any subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Covered Entity, agree to the restrictions and conditions which apply to the Associate hereunder.

m. **Amendments**. The Associate shall make available to the specific Individual to whom it applies any PHI; make such PHI available for amendment; and make available the PHI required to provide an accounting of disclosures, all to the extent

required by 45 CFR §§ 164.524, 164.526, and 164.528 respectively.

n. **Federal Access**. The Associate shall make its internal practices books, and records relating to the use and disclosure of PHI received from, or created or received by the Associate on behalf of the Covered Entity available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504.

4. **Termination**.

a. **Duties at Termination**. Upon any termination of this Agreement, if feasible, the Associate shall return or destroy all PHI received from, or created or received by the Associate on behalf of the Covered Entity that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Agreement to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents and subcontractors to assist the Covered Entity with any HIPAA required accounting of disclosures survives the termination of this Agreement.

b. **Termination For Cause**. Covered Entity may terminate this Agreement if at any time it determines that the Associate has violated a material term of the Agreement. Covered Entity may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.

c. **Survival**. The respective rights and obligations of Associate under Section 3.k. of this Agreement shall survive the termination of this Agreement.

5. **General Provisions/Ownership of PHI**.

a. **Retention of Ownership**. Ownership of the PHI resides with the Covered Entity and is to be returned on demand.

b. **Secondary PHI**. Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an Individual must be held confidential and is also the property of Covered Entity.

c. **Electronic Transmission**. Except as permitted by law or this Agreement, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses not authorized by this Agreement or to another contractor, or allied agency, or affiliate without prior written approval of Covered Entity.

d. **No Sales**. Reports or data containing the PHI may not be sold without Covered Entity's or the affected Individual's written consent.

e. **No Third-Party Beneficiaries**. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Associate and their respective successors or assigns, any rights remedies, obligations or liabilities whatsoever.