Section 14. Information Security Addendum

1. SwiftTech, herein referred to a Vendor, agrees to and warrants Greater Minnesota Lifecare, herein referred to as (Company), that Vendor will minimally complies with or exceeds the information security standards set forth below:

2. Vendor stipulates that, regardless of its relationship to Company, Vendor will meet the minimum acceptable standards for a healthcare provider or data processor that stores, transmits, or processes electronic personal healthcare information (ePHI) within the United States.

3. Vendor further stipulates that it will update its information security management policy at least quarterly or sooner if significant changes to operating policy, system, or security architecture changes warrant modification.

4. Vendor must use strong data encryption (e.g. AES-256 or stronger) to store all Company's information.

5. Vendor must ensure that all application code is tested and free of security flaws that would create risk greater than a rating of "low". Any security flaws that are risk rated as "High" (or equivalent) or "Medium" (or equivalent) using a standard, recognized risk rating mechanism must be remediated prior to the code being deployed to production environments.

6. Company shall have the right to perform an information security audit at any point during the term of this agreement so long as Company provides 30 days' notice to Vendor. Audit topics may include but is not limited to:

    a. Information Security Policy

    b. Information Security Risk Management Policy

    c. Risk Assessments

    d. Security Controls and Procedures

    e. SDLC

    …

    …

    …

12. Should Vendor fail to meet any obligation herein, Company shall have exclusive right to terminate this agreement in full following notice and a 15-day period in which Vendor shall have the opportunity to rectify any deficiency.

… end of excerpt