Section 14. Information Security Addendum

1. SwiftTech, herein referred to a Vendor, agrees to and warrants to 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:

i. An Information Security Policy shall be established to provide a comprehensive framework for protecting the organization's information assets and ensuring the confidentiality, integrity, and availability of data.

ii. The Information Security Policy shall define roles, responsibilities, and accountability for information security across the organization.

iii. All employees, contractors, and third parties shall be required to adhere to the Information Security Policy and its associated procedures.

b. Information Security Risk Management Policy:

i. An Information Security Risk Management Policy shall be implemented to identify, assess, and manage risks to the organization's information assets.

ii. Regular risk assessments and reviews shall be conducted to identify potential risks, evaluate their impact, and develop appropriate risk mitigation strategies.

iii. Risk acceptance criteria and risk treatment plans shall be established to guide risk management decisions and ensure alignment with business goals and compliance requirements.

c. Risk Assessments:

i. Risk assessments shall be conducted periodically to identify and evaluate potential risks to the organization's information assets, systems, and operations.

ii. The risk assessment process shall consider internal and external threats, vulnerabilities, likelihood of occurrence, and potential impacts.

iii. Findings from risk assessments shall be used to prioritize risk mitigation efforts, allocate resources effectively, and inform decision-making processes.

d. Security Controls and Procedures:

i. Appropriate security controls and procedures shall be implemented to safeguard information assets, systems, and networks.

ii. Access controls, encryption, monitoring, logging, incident response, and other security measures shall be deployed to protect against unauthorized access, disclosure, alteration, and destruction of sensitive data.

iii. Security controls and procedures shall be regularly reviewed, updated, and tested to ensure their effectiveness and compliance with industry best practices and regulatory requirements.

e. SDLC (Software Development Life Cycle):

i. A secure Software Development Life Cycle (SDLC) shall be implemented to ensure that security is integrated throughout the entire software development process.

ii. Security requirements shall be defined and incorporated into the software development process from the initial design phase to deployment and maintenance.

iii. Regular security assessments, code reviews, and testing shall be performed to identify and mitigate security vulnerabilities and ensure the delivery of secure software.

f. Data Storage Policy:

i. All sensitive data stored in VPC3 File storage shall be encrypted using strong encryption algorithms, such as AES-256.

ii. Databases in the production environment shall be encrypted to ensure the confidentiality of the data.

g. End-User Management Policy:

i. Internal network users shall be required to create and maintain passwords with a minimum of 7 characters to ensure password strength.

ii. Passwords for all users, including internal network users, shall expire periodically as per the password expiration policy.

h. Network Controls Policy:

i. VPN access to the organization's network shall require multi-factor authentication (MFA) to enhance security.

ii. The use of outdated protocols, such as TLS v1.1, shall be deprecated, and stronger protocols shall be implemented for secure communication between the cloud production environment and SwiftTech's physical location.

i. Vulnerability and Patch Management Policy:

i. Development Tier servers shall be regularly patched and updated to address vulnerabilities and ensure a secure environment.

ii. Regular vulnerability assessments and scanning shall be conducted on Development Tier servers to identify and remediate any potential vulnerabilities.

j. Code Scanning Policy:

i. All application code shall undergo thorough scanning and review for vulnerabilities before being deployed into the production environment to minimize the risk of introducing vulnerable code.

7. 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