Generation Health Vendor Assessment Report

Executive Summary:

Telemachus Cloud Services (TCS) is an Infrastructure-as-a-Service (IaaS) company that provides cloud services and hosting platforms to customers at a global scale. Customers may use TCS to host services that can be scaled across their customer base. TCS uses a shared responsibility model where TCS is responsible for the security of their physical infrastructure, while customers are responsible for the security of the applications they run on TCS.

TCS will have access to our patients' PII, PHI, and proprietary info. Given this fact, TCS must comply with HIPAA requirements. TCS' systems are hosted internationally, but Generation Health will require that all servers and data be hosted in data centers in the United States only. Even still, TCR must also comply with GDPR since it has its systems also hosted in E.U affiliated countries.

Our company plans to use TCS to accomplish the following: 1) host and scale our next-generation cloud platform; and 2) Manage the physical security and environmental controls, backup and restoration services, and provide infrastructure level monitoring and network security.

Assessment of Telemachus' Security Controls:

TCS has a formal process for managing system updates and security patches, but a recent security test found that some critical systems remain unpatched. Additionally, one of the five standard system setups used in their Customer Support Platform was also missing important updates, as noted in their SOC 2 Type II report. While TCS has strong encryption measures in place, they use multi-factor authentication (MFA) for most systems but not for their Customer Support Portal. Their security policy only requires two-factor authentication (2FA), which may not fully align with best practices. Another concern is their password policy, which requires a minimum of 8 characters, while security experts recommend at least 10 for stronger protection. Lastly, TCS does not back up key systems and data, relying instead on a highly resilient system design. This approach could pose a risk if unexpected failures or cyber incidents occur.

Risks:

1. If external parties get access to TCS through exploiting vulnerabilities, unpatched systems, and a lack of MFA enforcement in TCS' Customer Support Platform, then they will have access to our patients' PII and PHI which may create non-compliance with HIPAA - HIGH severity risk.
2. If there are natural disasters where the off-premise data centers are located it may create operational disruptions for our employees and significant concerns for our company due to a lack of scoped systems and data performed, this is a HIGH severity risk.

3. If external parties gain unauthorized access to TCS, they will have access to our proprietary info then it can create significant financial loss for our company - HIGH severity risk.

Recommendations:

Based on a review of TCS's security documentation, the company has inadequate security controls. We recommend the following actions:

1. IT should integrate TCS with Okta and enable Single Sign-On (SSO) with Multi-Factor Authentication (MFA) to enhance access security, protect sensitive patient data (PII and PHI), and ensure ongoing HIPAA compliance.
2. Legal should update the Master Services Agreement (MSA) to require TCS to implement a backup and data restoration process within 30 days to ensure business continuity and resource availability.
3. TCS should update its password policy to require a minimum of 10-character passwords while maintaining existing security requirements for stronger user authentication.