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.

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:

While TCS does have a formal change management and patching process in place, they have unpatched critical systems open per the Pentest. Additionally, it was noted that 1 of 5 of their standard system images was not patched on their Customer Support Platform per their SOC 2 Type II report. While they do have notable encryption protocols in place, they report using MFA on SIG Lite for most systems except customer support portal, but their password policy states they only require 2FA. Additionally, they list only a minimum of 8 characters in their policy whereas the Pentest report recommends a minimum of 10 characters. Lastly, TCS mentions that they do not implement backup of scoped systems and data performed stating they have a high resiliency architecture.

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 documentation provided by TCS, the company has demonstrated inadequate security controls. We have the following recommendations:

1. IT should integrate TCS with Okta and enable SSO with MFA to strengthen access control to protect PII and PHI to ensure continued compliance with HIPAA.
2. Legal to add a clause to the Master Services Agreement to require the vendor to implement backup/data restoration process to maintain availability of resources within the next 30 days.
3. Vendor needs to update password policy to require all users to create a password with a minimum of 10 characters with other necessary requirements kept the same.