**Risk Assessment Mitigation Report**

Management Signoff:

Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Management Signoff of Completion of Mitigation Items:

Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security topics that scored a MEDIUM or higher on the risk assessment were identified, and remediation steps were developed for any open items. A report of items needing mitigation are described below:

**Physical**

**PH23 - §164.310(c) Standard Does your practice have policies and procedures that describe how to position workstations to limit the ability of unauthorized individuals to view ePHI?**

We will purchase security stations for all workstations with ePHI access. In addition, we will continue to follow automatic log-off procedures for unattended workstations.

*Completed: 10/1/2016. Screens purchased from Amazon, confirmed installation by HG.*

**PH29 - §164.310(c) Standard Do your policies and procedures set standards for workstations that are allowed to be used outside of your facility?**

We will institute policies to use privacy screens for all workstations and prevent access to ePHI from outside locations to prevent unauthorized access.

*Completed: 10/1/2016, revisions confirmed by HG.*

*Policy was amended with the statement: \* Any workstations used to access ePHI are required to use privacy screens and be placed in office locations that minimize unauthorized viewing of information.*

**Administrative**

**A4 - §164.308(a)(1)(ii)(A) Required Does your practice periodically complete an accurate and thorough risk analysis, such as upon occurrence of a significant event or change in your business organization or environment?**

While we already periodically complete a risk analysis, this analysis will now be updated after:

• Large customer partnerships constituting order of magnitude changes in scale

• Any doubling of firm size

• Major software update to fundamental information systems used

*Completed: 10/15/2016; The risk analysis documentation was updated after determining the correct set of conditions for review. HG*

*Policy was amended to state:*

*5. Any doubling of firm size*

*6. Any major software update to core databases or server technologies used.*

*7. Any large customer partnerships consituting a 5x increase in customer volume.*

**A23 - §164.308(a)(3)(ii)(A) Addressable Does your practice have policies and procedures for access authorization that support segregation of duties?**

While RBAC is currently implemented using hard-coded permissions, we need to transition to more flexible authentication architecture to allow for us to add actions to the roles as the software expands in scope and use.

*Completed: 11/1/2016; A new authentication controller was released that more clearly ties roles to permissions both on the Node backend and the Angular front-end to allow for easier addition or removal of permissions from roles. Confirmed by OR, technical lead.*

**A39 - §164.308(a)(5)(ii)(A) Addressable As part of your practice’s ongoing security awareness activities, does your practice prepare and communicate periodic security reminders to communicate about new or important issues?**

We’ve set up a bimonthly security reminder schedule to ensure that reminders for security are sent to all those who have access to ePHI to follow proper security practices.

*Completed: 9/6/2016, Confirmed by HG*

**Technical**

**T3 - §164.312(a)(1) Standard Does your practice analyze the activities performed by all of its workforce and service providers to identify the extent to which each needs access to ePHI?**

\* We will structure pre-emptive reviews with health plans and business partners during the process of setting up a pilot process to ensure that we are aligned on the access controls and only create user accounts as necessary.

*Completed: 11/05/2016; A workflow step was added to all new pilot set up processes for health plan partners to submit an Access Review Request. The Access Review Request form is found here: https://docs.google.com/a/towerviewhealth.com/forms/d/1zz9WmWI36glvA3TLGN1-GzpUu3EccJXIgrB9Sq9fPHs/*

**T6 - §164.312(a)(2)(i) Required Does your practice require that each user enter a unique user identifier prior to obtaining access to ePHI?**

Ideally, we would use a SAML or SSO system to further vet the access through the existing IT infrastructure if applicable. We are exploring these practices for larger rollouts as integration resources become available.

*Completed: 9/17/2016; It was determined that a SAML system is not appropriate at this time for business partners as the integration process would require a larger scale rollout.*