Risk Assessment Mitigation Report

Security topics that scored a MEDIUM or higher on the risk assessment were identified, and remediation steps were developed for any open items. A summary of the topics 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.

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.

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 analyss, 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

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.

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.

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.

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.