PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

Information Security and Privacy Office

Partners HealthCare System, Inc.
Information Security Brief

System Name: MAPS

Version Number: 1.0
Report Date: February 8, 2018

Partners HealthCare Confidential Data
For Authorized Use Only

Request

MGH Recovery Research Institute requested a formal assessment to be conducted of their internally developed application, MAPS, in order to confirm compliance regulations and security best practices are met.

Background
The MAPS application is currently in development. It was created by an outside vendor, Freeelancer Erin Regan. She delivered a minimally functional prototype. Erin is not expected to perform further support for the product. Rather, Boston Tech, an outside vendor, has been engaged to complete development inot a fully functional application.

The use case involves a staff member accessing MAPS through an internal URL (phsweb2119.partners.org/survey/signin.php) and assigns the patient a study number. The staff member provides the ipad from which this was done to the patient who then completes a survey that was opened. The patient clicks submit and gives the ipad back to the receptionist.

All access to the data collected is only available to back office staff. This is a web app that is hosted on PHS data centers. It cannot be accessed from non-phs networks. The survey number and question answers are the only data input. The FN, LN, DOB, Clinician and Appointment date are kept on a database not available to the patient, but correlated to the patient on the database.

Access roles are (a) Survey Administerer (not Administrator) i.e. a staff role who gives out the survey, (b) Clinician (c) Director. The web application is on server phsweb2119.

Boston Tech has the capability to complete their work in their own environment if given the source code and certain configuration information. Once development and testing is complete the program will reside on phsweb2119.

Information Security's Recommended Action(s)
After reviewing the application and its existing security controls, the risks identified are based off of internal policies and best practices. The Information Security department then recommends the following:

1. Create a log review process to go over any and all captured logs and its events.
2. Engage with the SecEng team and scan server phsweb2119 using Tenable, this will allow us to have an accurate and up to date documentation in regards to the server vulnerabilities and then plan any required remediation.
3. Ipads (or any other mobile devices) used for surveys must conform to PHS mobile device standards.
4. We recommend that a Formal Account provisioning, review and termination procedure be put in place.
5. We recommend that access controls such as inactivity timeouts, failed login lockouts and all other PHS build requirements be included in the final MAPS application.
6. Work with web operations – phs in order to gain the support necessary to provide Boston Technology with copy of current implementation, snapshot of system, backups and other files needed for Boston Technology to complete development of MAPS from their environment without direct access to PHS.
7. Patient data entered into MAPS should be encrypted at rest.

8. Prior to being placed into production, MAPS should be scanned by Veracode and any findings remediated.