

Sprint Planning Meeting Minutes: Sprint 4

Project: **FIU Doctor Booking System**

Attendees: Mohammad Kazmi, Jason Eduardo Kildare, Wenjia Wang (PO)

Start time: 9:00 AM

End time: 9:30 AM

After discussion, the velocity of the team was estimated to be **60 hours for the team**.

The product owner chose the following user stories to be done during the next sprint. They are ordered based on their priority.

- **User Story #1:** As a developer, I want to implement a log of all accesses and changes to electronic protected health information to keep track of unauthorized access or alterations. **164.312(b) (Security Rule)**
- **User Story #2:** As a developer, I want to limit the number of unsuccessful login attempts in order to prevent unauthorized access to a patient or a doctor's account. **164.308(a)(5)(ii)(C) (Security Rule)**
- **User Story #3:** As a developer, I want to make the users/doctors conform to an agreement when they register their account ensuring that their medical health information is protected, but it can be used if required by verified medical personnel or law and that they refrain from illegal activities on the app. **164.308(b)(3) (Security Rule)**
- **User Story #4:** As a developer, I want to implement procedures for monitoring log-in attempts such as the time and place where the account was logged in and report/notify the patient if it was logged in from a different location. **164.308(a)(5)(ii)(C) (Security Rule)**
- **User Story #5:** As a developer, I want to implement an automated notification system both in-app and email to notify the user in the event of a breach. **164.404(a) (Breach Notification Rule)**
- **User Story #6:** As a user, I want to receive any digital verification or proof of the doctor before disclosing any personal health information to the doctor. **164.514(h) (Privacy Rule)**
- **User Story #7:** As a developer, I want to scan files(PDFs, JPGs) which can be medical documents/records uploaded by the users or digital verification/proofs uploaded by doctors for vulnerabilities to ensure the files uploaded to the system are safe. **164.308(a)(5)(ii)(B) (Security Rule)**

- **User Story #8:** As a developer I want to implement a feature to ensure that access privileges are immediately denied to terminated workforce members. **164.308(a)(3)(ii)(C) (Security Rule)**
- **User Story #9:** As a developer I want to prohibit users from reusing previously used passwords. **164.308(a)(5)(ii)(D) (Security Rule)**
- **User Story #10:** As a developer, I want to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. **164.312(a)(2)(iii) (Security Rule)**

The team members indicated their willingness to work on the following user stories.

- **Mohammad Kazmi**
 - **User Story #2:** As a developer, I want to limit the number of unsuccessful login attempts in order to prevent unauthorized access to a patient or a doctor's account. **164.308(a)(5)(ii)(C) (Security Rule)**
 - **User Story #3:** As a developer, I want to make the users/doctors conform to an agreement when they register their account ensuring that their medical health information is protected, but it can be used if required by verified medical personnel or law and that they refrain from illegal activities on the app. **164.308(b)(3) (Security Rule)**
 - **User Story #4:** As a developer, I want to implement procedures for monitoring log-in attempts such as the time and place where the account was logged in and report/notify the patient if it was logged in from a different location. **164.308(a)(5)(ii)(C) (Security Rule)**
 - **User Story #6:** As a user, I want to receive any digital verification or proof of the doctor before disclosing any personal health information to the doctor. **164.514(h) (Privacy Rule)**
 - **User Story #7:** As a developer, I want to scan files(PDFs, JPGs) which can be medical documents/records uploaded by the users or digital verification/proofs uploaded by doctors for vulnerabilities to ensure the files uploaded to the system are safe. **164.308(a)(5)(ii)(B) (Security Rule)**

- **Jason Eduardo Kildare**
 - **User Story #1:** As a developer, I want to implement a log of all accesses and changes to electronic protected health information to keep track of unauthorized access or alterations. **164.312(b) (Security Rule)**
 - **User Story #5:** As a developer, I want to implement an automated notification system both in-app and email to notify the user in the event of a breach. **164.404(a) (Breach Notification Rule)**
 - **User Story #8:** As a developer I want to implement a feature to ensure that access privileges are immediately denied to terminated workforce members. **164.308(a)(3)(ii)(C) (Security Rule)**
 - **User Story #9:** As a developer I want to prohibit users from reusing previously used passwords. **164.308(a)(5)(ii)(D) (Security Rule)**
 - **User Story #10:** As a developer, I want to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. **164.312(a)(2)(iii) (Security Rule)**