BROAD INSTITUTE | CLINICAL RESEARCH SEQUENCING PLATFORM

Box security: FAQ

Broad has made a decision to allow for a "write-only" upload area in Box. This uses File Request in Box that allows a user to submit one or more files with metadata which is stored in a private folder owned and accessed by a limited list of Broad personnel.

This is similar in function to a "bank night deposit slot" or USPS Mailbox. Users will ONLY be able to see their own data and data will NOT be able to be overwritten. There is no risk of loss of confidentiality with this setup.

We made this decision to have unauthenticated upload because we believe that managing the credentials and accounts for hundreds of users coming from an outside source will be costly and time-consuming -- especially since the only functionality is upload. We will be asking users to include an institute-specific ID to help verify the uploads.

Users uncomfortable with having an open-upload location can contact the Broad to discuss authenticated options. There might be an additional charge for that.

We made the choice of using Box as opposed to standing up our own site because of their well-known security posture.

How will the data be protected after it has been uploaded to Box?

Data in Box will be rosters that will populate some of our automated systems at Broad. It will be accessed by service accounts or by a limited number of Broad users. We will be purging data at the close of the contract.

For general security of our COVID pipeline, see the following.

Is there 2FA on the Box account?

For admin/read access to the Box, all Broad personnel use 2FA from their GSuite SSO accounts. Broad has a robust SIEM/SOC environment and accounts are monitored 24/7.

Is there a signed BAA with Box?

BAAs (Business Associate Agreements) are only for Covered Entities and Business Associates as applied to HIPAA. We are neither so we do NOT have BAAs. However we have security agreements that are similar and we ourselves abide by the Security and Breach rules in HIPAA.