Smart Chart Security Document

1. How personal data is transmitted/ communicated.
    a. All login and registration information that is sent from the user to the system/database is hashed using SHA1 before transfer to prevent any simple sniffing or man-in-the middle attacks. No login or account information is transmitted in plaintext, safely concealing all of the user's information.
2. How personal data is stored.
    a. The personal information is also held in the database using the SHA1 hashing function. This will make login fairly straight forward and so that no plain text information will have to be sent over the network. Information will be hashed client side and then sent to the database to be compared to the hashed entry. This will also assure that any break in security of the database will not reveal plaintext passwords to the unauthorized subjects.
3. How external system data is stored.
    a. There are not external systems that our system uses that would require security of any passwords or API keys, so this section of the Document is not needed for our application.
4. Before/After deployment.
    a. The methods of data transmitting and storing are the same before and after deployment of the application.