**What makes up a Desirable mHealth App?**

mHealth apps have revolutionized the healthcare industry with their multiple benefits to patients and doctors, allowing them to benefit from healthcare facilities beyond hospital premises. Development and usage of mHealth apps has doubled in the past two years, and developers are striving to provide apps that follow best practices to completely cater to the industry needs. With increased competition in the app market, organizations now have to choose options that are best-suited to their needs. As outlined by FTC, healthcare stakeholders should look for the following features when choosing mHealth apps:

1. **It should collect only required data**. According to the recommendations of FTC, mHealth apps should collect only that data which is vital for delivering a product or service. Also, an app that is well developed should be able to secure, store, send, receive and delete the data.
2. **It should only allow limited access.** Rather than direct API access, a well-designed app will use a trusted interface to avoid unnecessary app permissions and to limit access. App permissions should only be used when required, to minimize the collection of unrequired data.
3. **It should provide secure authentication.** Healthcare records are not only important for patients and doctors, they are also significant to hackers for extracting useful information. Apps that provide secure authentication are trusted more by all stakeholders and secure authentication should be a primary concern of developers. App authentication should be designed, implemented and tested for security from the very beginning. In case of higher risk factor, two-factor or multi-factor authentication needs to be considered.
4. **It should be compatible for all platforms.** Mobile platforms differ in app permissions, security features and API. A good app will work to ensure the protection of user data regardless of the platform.
5. **It should have room for security improvement.** Software libraries, cross-platform toolkits, software development kits (SDKs), etc. are available for improving application-level security. These can be used to check password strength, improve encryption, test interfaces, direct pre and post launch testing and reverse engineer program code.
6. **It should clearly communicate with the users.** Before any information is required from the patient, a well-designed app must clearly communicate all terms and acquire consent before and after installation. A much better approach would be to include a privacy policy that can be easily read and understood by the users.
7. **It must comply with the regulations.** Though it will be a challenging task for the developers, yet an app should comply with all healthcare regulations such as HIPAA, FTC Act, FTC Health Breach Notification Rule, etc.

The year 2017 will provide exciting opportunities for development of mobile health technology and mHealth apps and wise developers need to review best practices closely in order to develop the most compliant and trusted apps.