Data Security and Privacy on iStayHealthy

February 9, 2012 By iStayHealthy

Many of you asked questions or expressed concerns regarding data stored in iStayHealthy. I take this issue very seriously. From my point of view there are two main aspects to it: a.) the concern that others may find out about my HIV status; b.) the data on the phone may be abused.

The first aspect is obviously a grave concern. HIV is still widely stigmatised. And having an application on your mobile device that spells HIV can lead to others finding out about your status. Just imagine you are showing off your shiny new iPhone/Android device at a family gathering...

The second one is no less serious. There are a number of baddies out there who just wait for us to reveal our secrets, identity. Maybe not so much to access our health data, but to use private data (such as e-mail accounts etc) for identity theft.

When designing the app I implemented a few safeguards, that should protect you under most circumstances. But let's first deal with what is actually happening with iStayHealthy 'under the hood'.

The more technically savvy may already know that application data on iPhones/iPads and Android devices are "sandboxed". What this means is that by default the application itself - and only the application - can access the data. Apps can be designed to share their data. But this is not a design I implemented for iStayHealthy.

Secondly, the data are not shared and secretly sent to anywhere or anyone. There is no secret data mining that sends the data to some other party. The data in iStayHealthy are YOUR data and no one else's. You decide if you want to e-mail the results to someone else. You decide if you want to backup/restore it to/from Dropbox.

However, I do realise this may not be enough to protect you from unwarranted users finding out about you and your status. To address this I implemented a password protection for iStayHealthy from version 3 onwards. You can access the data in the app only if you type in the password - otherwise only the home screen with no data is shown.

There is another important measure you can take to protect your phone and your data (not just iStayHealthy) from prying eyes. And this is to use the key-lock mechanism. When you enable this feature (usually in the device Settings menu) you will have to provide a 4 digit pass key.

© 2026 Smart + Strong All Rights Reserved.
http://beta.docker.poz.com/blog/data-security-and-pr