Q and A on Weatec Security:

Who has access to my data?

You, your local WMRC person, your Weatec deacon, the Weatec administration committee, and in some cases, your home deacon. Also see section below on “What about developers and helpdesk personnel?”.

What data is stored?

To provide accountability, Weatec collects usage details of the websites you visit and the apps you use. For apps we typically get the app name and a clip of text from the screen. There is a user adjustable setting that determines which apps we can get these ‘text clips’ from. Weatec requires monitoring for most apps. There are some banking and messaging type apps that Weatec considers private. Weatec will not record any usage details from these apps. We also record the amount of time spent in all apps. For websites we typically collect the website address (URL) and the wording that shows in the browser tab (page title).

While Weatec does store personally identifiable information, the type of data we store is not what your typical hacker would really want. Example: we don’t store the type of data that could cause a financial loss or personal hardship if a rouge person would somehow get access to it.

What about: social security numbers, credit card info, bank account info, passwords, etc. How likely is it that this info would be recorded in the Weatec system?

This is very unlikely. Most quality apps use special precautions for sensitive information and there is no possible way for us to get that info if we would want to. On the other hand, we are trying hard not to record any such info. If such data was recorded, it is still covered by the security features Weatec has in place to protect all data.

How long is usage data kept?

Usage data is kept for maximum of 6 months. After that it is deleted.

What about developers and helpdesk personnel?

At times it may be necessary for developers and helpdesk personnel to access the system. These people have special permission from Weatec to do so. They are under a confidentiality agreement that dictates they shall only access the usage they need to complete their job. Weatec has procedures in place to make sure such access is reduced to an essential minimum.

What is Weatec doing to mitigate the risk of being hacked?

Weatec uses standard industry practices to secure data in transit as well as stored data. Traffic to and from the servers is encrypted.

Is there anything users can do to help reduce risk of something bad happening?

All users have access to their own usage details. Use the Weatec app or website to get familiar with the type of usage details we collect. Ever Accountable and Security Appliance also have their own reports that you may want to review.

For devices using Ever Accountable, review your monitored apps settings. Turn off monitoring for banking apps, password managers, and email apps. Please keep monitoring turned on for all other apps. The system will flag if monitoring is turned off for apps that require monitoring. See website for more details on these settings.

Make sure you are using the most up-to-date version of Ever Accountable or Security Appliance MDM.

Review the setup tips for your type of device iOS or Android.

If you have additional questions or concerns please contact us:
wmrc@weatec.com | Call or text: 717-690-0006 | https://weatec.com/