KALEIDOS and KALEIDOS plus GDPR compliance

In Adaptica we care about data. We protect your data and the data of your clients.

This document explains the privacy and security features of KALEIDOS and KALEIDOS plus and gives hints on how to further improve the security of the data.

KALEIDOS and KALEIDOS plus security features

KALEIDOS and KALEIDOS plus are both composed by a 2WIN-S and a control tablet running KALEIDOS App. These are the features and specifications regarding the security of the data stored into the two devices.

- The 2WIN-S performs only anonymous examinations, so no personal data are stored in the device.
- In the KALEIDOS App it is possible to insert patient data (available from software version 5.4). These data are not sent to the 2WIN-S and are kept inside the control tablet.
- KALEIDOS App will work only if a security lock is set up in the control tablet. The app will warn the user if the security lock is not set and it won't startup until this is set up.
- The AI application (available from software version 5.5.0) sends and stores only anonymous data and the minimum amount needed for service, if necessary.
- EMR integration (available from software version 5.5.0) requires the user to set up a shared folder. This must be done with the samba protocol and requires that a password is set on the shared folder.
- Only one examination at the time is saved in the shared folder, in order to avoid multiple examinations not under direct control by the application.

Hints in order to improve the security

In order to improve the security of the data the following actions are strongly recommended.

1. Encrypt your control tablet with a safe ID or password.
   KALEIDOS plus comes with a dedicated Remote Console, which is already encrypted with a default password. But we would like you to set up your password, so only you can access your data. In case the device is stolen this would prevent strangers to access the data inside.
   Choose a proper security screen lock, such as an ID with at least 6 numbers or a password of at least 8 characters including capital letters numbers and symbols.
2. The same advice for the password it is true to protect the EMR shared folder.
3. To secure the EMR shared folder, upgrade regularly the PC or server from which the shared folder is set up with the latest OS security patches.