INVie™

Data Security
Overview

INVie™

Data security at a glance

INVie incorporates **strong** data security **features**. As a **standalone** system, the **risk** of vulnerabilities and threats to INVie's data and connected systems is **essentially non-existent**. The **consequences** of an unlikely data breach are **negligible**, as the data is of **little value** to any outside party. INVie is used only in **access-controlled** areas, and there is **no anticipated** use of financial, sensitive, or protected health information (**PHI**) within INVie.

Restricted account access

- Only the facility's IT department will have access to the Apple ID login
- End-users interacting with INVie are prevented from accessing the data elsewhere

Protection from theft

- All devices will be locked using the iOS passcode which is only known to the facility's IT department
- Physical access to the device will not allow access to the database or Apple ID account

Always locked

- All devices will be locked on INVie, meaning no other apps or software can be used

Apple iCloud services

- INVie data is synced on battle-proven platform with over 700 million users and no known security breaches in its history

Idle timer and auto-logout

- INVie will revert back to its default state and log out any Approvers when idle

Encryption

- All data is **encrypted** on device through the iOS **passcode**
- All data is encrypted during **transmission** and on the server with a minimum **AES-128** encryption

Password protected

- All INVie accounts are protected with a salted and hashed passcode and password

Privacy

- activeHX **cannot** access or manipulate user-created data unless provided access to the Apple ID account or device