General FAQ's

General FAQ's

Does the system require the internet to operate?

Yes & No! - The collector unit does require internet to relay the alerts to the cloud site but this is for reporting data only. The mobile app does **not** rely on the actual internet to receive an alert, the smart devices within the home communicate locally to the collector unit connected to the Nursecall system and alerts are delivered to the mobile devices over the local Wi-Fi.

If a loss of internet occurs, then messages are simply queued on the collector locally until the internet becomes operational and any alerts are back-fed to the cloud site.

How does the mobile app store data and what protection is in place to avoid unauthorised access to our data and/or our network through the app

We use an OAuth API between the app and the collector on site, with each user only being permitted one session at a time (if a user logs in to a second device, the first session is terminated automatically). All API endpoints require a valid token in order to make any requests, and we only accept authentication request from our own OAuth clients embedded into the mobile application.

Data is cached locally within the app for the user to interact with alerts, send messages to colleagues and set their user preferences. This data is also stored on site in the collector within a local database.

Where is the data stored for use of the Mobile App

The primary store for data presented in the app is in a database on the collector within the care home. The mobile app does not, at any time, communicate with our cloud platform or any location on the internet. All communication is done locally within the care home.

How is local data relayed to the cloud platform

The data is relayed to our cloud platform over an encrypted WireGuard tunnel and stored within a private network in our database cluster.

If for any reason, the WireGuard tunnel is interrupted then all data is kept cached locally until the tunnel connection is restored. This data does not go over the open internet.

We run a separate process within the collector to securely send alert data and information to our cloud platform for analysis and to then relay to third parties (such as PCS, Nourish and Care Control) if the care home has opted in to this and it has been configured.

> How long is the data stored in Cloud

We do not routinely delete this data, with the intention that it is essentially stored forever, provided the care home is a customer with us.

Should a home choose to discontinue their service with us, our development team are informed, and we remove all data from our live database cluster within 24 – 48 hours and it is rotated out of backups within three months.

> € Are copies of the database taken

We do not actively back up data within the collector as this is synchronised to/from the cloud platform, so if a replacement is required it can be activated and the configuration data and users are pulled down from the cloud automatically.

We back up our cloud platform database every thirty minutes and keep three months stored in a private and encrypted storage bucket our cloud storage provider Wasabi

> I would like to see more on the risks of data tracking and permissions. Our devices collect a lot of information about us that is considered “sensitive” by major data protection legislation such as the General Data Protection Regulation (GDPR).

We do not collect any telemetry data about the user other than what is strictly necessary to provide our services. For example, if the user accepts an alert within the app, we store this timestamp and a unique identifier for that user, so we know who has chosen to accept the alert and we can show this in the reports on our cloud dashboard.

Data is **always** encrypted at least once while in transit.

Our database cluster is inaccessible via the internet, and we use strictly key-based authentication in order to access all servers across our fleet.

> We’re looking for more information on login protocols such as single sign on, password requirements, how long are accounts logged in for before timing out.

Single Sign On

We do not currently support SSO in either our web app or our mobile app. It is something that we have discussed in the past but have not yet implemented.

Password Requirements

For the cloud application we require passwords are a minimum of 8 characters long as length is ultimately the only way to ensure passwords are secure as the cloud application is available on the open internet. We also rate limit failed login attempts automatically to prevent brute force attacks.

For the mobile app we do not have any password requirements at this time as the scope for this is very limited (these users are only created for use in the mobile app and are only available to login to by being present within the care home using a device with the application installed)

- How long are accounts logged in for before timing out

For our cloud-based web application we have a 120-minute session timeout, any page loads (or automated refreshes of the dashboard and other elements) will reset this timer. If the user opts to “Remember Me” upon login then their session will remain active until they log out regardless of the 120-minute timer

- I would like to see more on the risks of data tracking and permissions. Our devices collect a lot of information about us that is considered “sensitive” by major data protection legislation such as the General Data Protection Regulation (GDPR).

We do not collect any telemetry data about the user other than what is strictly necessary to provide our services. For example, if the user accepts an alert within the app, we store this timestamp and a unique identifier for that user, so we know who has chosen to accept the alert and we can show this in the reports on our cloud dashboard.

Data is **always** encrypted at least once while in transit.

Our database cluster is inaccessible via the internet, and we use strictly key-based authentication in order to access all servers across our fleet.

- Is data shared with any third parties and for what purpose

We do need to share some data with some third parties to deliver our service, but this is always kept to a minimum and is only when necessary. A list of third parties and what we use them for is below

Google – we use Google Play to distribute the application so basic app usage and installation information is sent to Google. We do not send any identifying data to Google for this purpose, but you are best reviewing their privacy policy to see what they collect. We also only support Android which is a Google operating system.

Microsoft – we use Microsoft Clarity for analytical purposes to build a better application, so some data is shared with Microsoft for this purpose. **Any information outside of the scope of what is strictly necessary to gather usage information about the application is censored and removed.**

Postmark – we use Postmark to send emails, so we need to send them the user's email address and the content of the email.

Wasabi – we Wasabi to store images, PDF versions of reports and our database backup data.

PCS – If the PCS integration is enabled, a summary of each alert is relayed to PCS for use by the care provider

Nourish – If the Nourish integration is enabled, a summary of each alert is relayed to Nourish for use by the care provider

Care Control – If the Care Control integration is enabled a summary of each alert is relayed to Care Control for use by the care provider

Kare-Inn- If the Kare-Inn integration is enabled a summary of each alert is relayed to Kare-Inn for use by the care provider

Other than this all-other infrastructure is operated by us, managed by us, and is secured by us. We use Hetzner Public Cloud as an infrastructure provider, but they do not have access to our data.