Google Play Data Safety Disclosure

The Alexys Mobile Application is an enterprise application used by authorised staff of healthcare organisations using the Alexys Aptus Critical Messaging System.

Data Collected

Depending on the configuration established by the healthcare facility, the App may collect and process the following information:

Data Type	Purpose
Approximate and Precise Location	Delivery of location-aware workflows, emergency response, staff safety, and operational reporting during authorised work activities.
User Identifiers	Authentication, message delivery, and user account management.
Device Identifiers	Device registration, system security, and reliable message delivery.
App Activity	Message acknowledgements, application diagnostics, and operational reporting.
Diagnostic Information	Troubleshooting, performance monitoring, and system reliability.

How Your Data Is Used

The information collected is used solely for:

- Delivery of critical clinical and operational messages.
- Staff safety and emergency response.
- Operational workflow and reporting.
- System administration.
- Technical support.
- Maintaining application security and reliability.

The App is **not used for advertising**, **marketing**, or **user profiling**.

Data Sharing

Information may be shared only with:

- the healthcare facility operating the Aptus system;
- authorised system administrators;
- authorised Alexys support personnel where required to provide technical support;
- trusted service providers acting on behalf of Alexys under confidentiality obligations.

Alexys does **not** sell personal information to third parties.

Security

Data transmitted between the App and the Aptus system is protected using industry-standard encryption during transmission.

Access to information is restricted to authorised personnel.

Data Deletion

Data processed by the App forms part of the healthcare facility's operational records.

Requests to access, correct, or delete information should be directed to the healthcare facility that issued the device, as the facility determines how data is retained and managed.

Device Permissions

The App may request the following Android permissions, depending on how the healthcare facility has configured the application:

- **Location** – to provide location-aware messaging, emergency response, staff safety, and operational reporting.
- **Notifications** – to receive critical clinical and operational messages.
- **Network Access** – to securely communicate with the Aptus system.
- **Foreground Service** – to maintain reliable message delivery and, where enabled, location updates while on duty.

The App does not access personal contacts, photos, videos, personal messages, call history, calendars, microphone, or camera unless those capabilities are explicitly introduced in a future release and disclosed accordingly.