

Alairo AMP Privacy Policy

Effective date: August 25th, 2026

Version 1.1

Summary

Alairo AMP is a hospital work app. A hospital assigns it to staff on a managed iPhone. Alairo AMP shows nurse-call alarms and messages, can play a notification when the app is in the background, and can place a voice call back to a room. The hospital chooses who uses Alairo AMP and hosts the AMP backend. Alairo provides the app. Apple and Google deliver push notifications.

This notice describes the information Alairo AMP handles when hospital staff use the app.

Who we are

Alairo Solutions, LLC ("Alairo," "we," "us," or "our") provides Alairo AMP. Alairo is a wholly owned subsidiary of Lone Star Communications, Inc. ("Lone Star").

This policy covers the Alairo AMP mobile app and the AMP services that support it. Hospital systems, device management, and network practices belong to the hospital customer.

How AMP is used

A hospital customer assigns Alairo AMP to authorized staff, usually on a hospital-managed iPhone. The hospital controls the backend connection, the device identity, room and bed assignments, alarm behavior, and optional features.

The hospital may send that configuration through its mobile device management system. If it does not, a staff user can scan a hospital-provided QR code. Alairo AMP stores the working configuration on the device.

The hospital-assigned device ID is a work identifier. Alairo AMP never receives the staff user's Apple Account credentials.

Staff users should ask hospital IT, privacy, or compliance about hospital operational data. Alairo can help the hospital respond to a verified request.

Information AMP handles

Depending on hospital configuration, Alairo AMP may handle:

- Hospital backend address and feature settings
- Hospital-assigned device ID and optional staff extension
- Alarm and message identifiers, type, priority, status, and time
- Unit, room, floor, and bed identifiers
- Staff actions such as acknowledge, decline, answer, or message completion
- Free-text operational messages. These are notes a staff member types and sends to a specific phone, apart from coded nurse-call alarms such as Code Blue or Bathroom
- A push notification token and whether iOS allows Critical Alerts for Alairo AMP
- Microphone audio during a room dialback call
- A camera image used only to read a setup QR code
- A live room image or video stream, if the hospital makes that feature available and the staff user

turns it on

- Diagnostic information after a crash or when an authorized hospital administrator requests it
- Contact details and a message, if someone writes to Alairo or Lone Star for support

Alairo AMP's standard alarm fields are operational identifiers. A hospital can still put other details in a free-text message or a connected system feed. The hospital controls that content.

Alairo AMP does not create a consumer profile. It does not ask for a personal email, password, or Apple ID. It does not use Location Services, contacts, calendars, HealthKit, personal photos, or the advertising identifier. It does not show ads or sell AMP data.

How that information is used and shared

Alairo AMP uses this information to show current work, play configured sounds, avoid duplicate alerts, send staff actions back to the hospital, place dialback calls, and help authorized support staff diagnose delivery problems.

If notifications are allowed, the hospital AMP backend may send a push through Google Firebase Cloud Messaging. Apple then delivers it through Apple Push Notification service. An alarm notification can include the alarm type and location. A message notification can include a short excerpt of the text. iOS can show that title and body on the lock screen.

Alairo holds the production AMP Firebase project. A request to delete a Firebase installation goes to Alairo. A request to delete hospital backend records goes to hospital IT.

For an answerable alarm, Alairo AMP may place a voice call through hospital-controlled voice systems. The app asks for the microphone during that call. Alairo AMP has no call recording or stored audio.

When a QR code is used for setup, the camera image is used to read the code, then discarded.

If the hospital makes other Alairo features such as Insights or AFP available, a staff user can turn the live image or video feature on or off in the app. Alairo AMP can display the stream. It has no record, save, or upload control for that video.

A diagnostic bundle sent to the hospital backend can include app version, device ID, connection and permission status, and redacted recent logs.

Alairo AMP data may be available to:

- The hospital customer and people it authorizes
- Google, for Firebase Cloud Messaging
- Apple, for notifications, iOS permissions, and private app distribution
- The hospital's MDM provider, to assign and configure the app
- Lone Star, as Alairo's parent company, when authorized people help support AMP
- Authorities or other parties when disclosure is required by law

Google and Apple also process some device and service metadata when they provide those platform services, which can include an IP address.

Alairo AMP uses Firebase Cloud Messaging. It does not use Firebase Analytics, Firebase Crashlytics, Sentry, or an advertising SDK.

Retention, choices, and requests

The app keeps recent alarms and messages on the iPhone for a short time so staff can see current work. A message that arrives by push while the app is closed can stay on the device until the app is opened again.

Device configuration and related local records stay until Alairo AMP replaces them, the hospital resets the app, or the app is removed.

The hospital AMP backend keeps current operational records, push tokens, and device assignments so Alairo AMP can deliver work. Those hospital records stay until hospital IT or the hospital's retention process deletes them. Apple and Google retain information under their own terms.

Staff users can change notification, Critical Alerts, camera, microphone, and Local Network permission in iOS Settings. Denying Local Network access can block Alairo AMP from reaching a hospital backend on a private network.

Alairo AMP has no consumer account and no in-app account deletion control. Hospital IT can change assignments, replace configuration, or remove AMP from a managed device.

For hospital operational data, contact the hospital first. For a question about this policy, use Lone Star's contact page at <https://lonestarcom.com/overview/contact-us/>. Identify Alairo AMP, the hospital, and the hospital-assigned device ID if known. Do not include patient or alarm details in the public form. That page collects the name, company, email, phone, and message fields shown there.

Security and updates

Alairo AMP limits data to its work purpose and relies on iOS permissions and the hospital's devices, network, and hosted services. Transport security depends on the hospital's configuration.

A staff user who believes a managed device or AMP connection may be compromised should stop using the affected feature and report it to hospital IT.

Alairo AMP is a hospital staff work app. Alairo authorizes only hospital-assigned staff users. The hospital controls whether operational data relates to a pediatric care location.

We may update this policy when Alairo AMP's features, providers, or legal requirements change. We will post the revised policy at the same public URL and update the effective date.

Contact

For hospital operational data, contact the hospital customer's IT, privacy, or compliance team.

For this policy or an Alairo AMP privacy request:

<https://lonestarcom.com/overview/contact-us/>

State that the request concerns "Alairo AMP privacy."