HipLink Mobile

Solution Overview

This whitepaper gives a 360 degree overview of the HipLink mobile application solution. The HipLink Mobile App and HipLink communication server from HipLink Software provide an infrastructure for any organization that delivers alerts and notifications in real time with capabilities to support business messaging workflows and M2M communication.

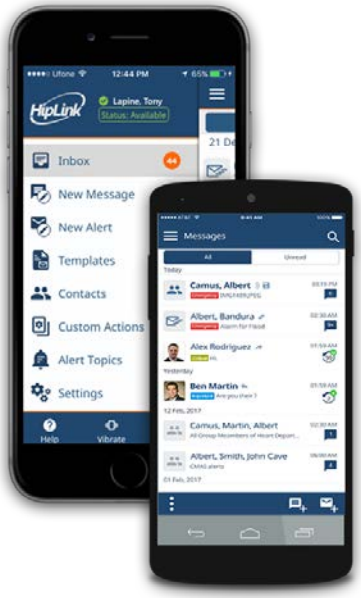
HIPLINK MOBILE APPLICATION - SOLUTION OVERVIEW

ABOUT THIS WHITEPAPER

This whitepaper describes the HipLink Mobile App solution for enterprises and organizations. The document provides a 360 degree overview of the solution and its offerings. It provides vital information to managers, executives, and decision makers to help them understand their business requirements for mobile notification, and how the HipLink offering can add value for their work environments.

INTRODUCTION

The workplace continues to move at an increasingly faster pace requiring real-time response and access, as well as secure text messaging. Smartphones can help bridge the technology gap for mobile employees as well as those that are just away from their desk or needed to respond during and after-hours.

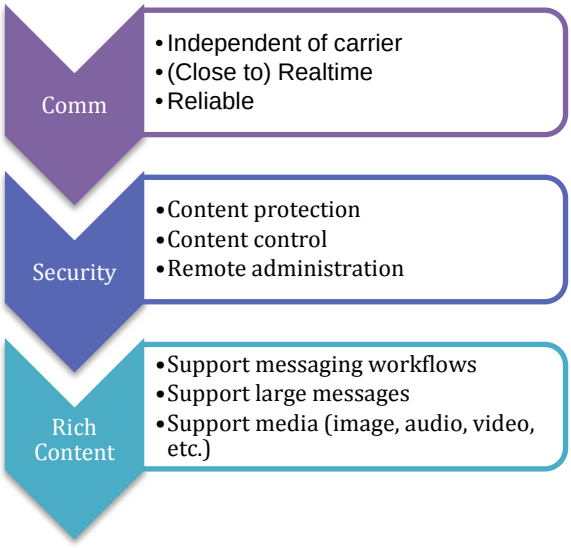


HipLink Software has developed the HipLink Mobile App that sends and receives alerts, enables M2M communication, and executes custom actions. All communications to and from the app are secure.

HipLink leverages its proprietary HipLink Notification Protocol (HNP) to work over the TCP layer with a live IP connection. This is completely independent of cellular SMS services. The application provides advanced messaging features for encrypted text messages, overriding phone settings for emergency messages, and one click responses from receivers. The HipLink mobile app is secure, easy-to manage, and improves overall communication throughout an organization regardless of location.

REDEFINING MOBILE NOTIFICATION FOR ENTERPRISES

Traditionally Mobile Notification services depended on the carrier and were often affected by carrier coverage limitations. The total cost of communications can be high because of carrier charges. Moreover, carrier based notification solutions provide basic (rudimentary) functions which lack support for content security, content type and size variety. Generally, 2-way workflow support is limited with dependence on a carrier. Traditional carrier-based messaging is not real time and can be unreliable with no proof of delivery.



HipLink Mobile provides a cutting edge platform for the enterprise that is unique from other solutions. It frees the customer from the carrier dependence on SMS text by allowing for communication over the Internet using Wi-Fi or carrier data networks. Along with it, the solution provides complete end-to-end security of messages with support for remote administration, and device control.

Above all the solution gives real time messaging services that can failover to SMS as a backup. The solution also enables advanced messaging workflows which are demanded by modern day enterprise environments.

One Solution for All Platforms

The HipLink Mobile App is available for the following platforms:

- Android smartphone
- Apple iPhone and iPod
- Microsoft Windows desktop

The solution is designed such that all platforms would support similar set of features. This enables an Enterprise to work with heterogeneous mobile devices and platforms.

Following is the list of supported platform operating systems:

Platform	Operating Systems
Android	Android 4.4 and above
iOS (Apple)	iOS 10 and above (works with 8 and 9 as well but with limited functionality)
MS Windows Desktop	Windows 7, Windows 8 and Windows 10

Easy to Adopt

The HipLink Mobile App is easy to adopt. Being compatible with various mobile platforms, it can easily replace an existing messaging system and can easily integrate the existing Enterprise infrastructure using HipLink's powerful SOAP APIs, and Response Actions. Furthermore, HipLink provides round the clock support making sure the customer gets the best out of the solution in least amount of time.

PROMOTES BYOD "BRING YOUR OWN DEVICE" USAGE MODEL

The solution allows for a BYOD model in the workplace by providing compatibility with commonly used mobile platforms. HipLink Mobile is easy to distribute and install and requires access to minimal device controls. This makes the solution's adoption an easy process.

The solution provides an easy registration process with optional manual authorization mechanism to control app installations.

USER INTUITIVE DESIGN & FUNCTIONALITY WITH EASY TO USE INTERFACE

The HipLink Mobile app offers an easy to grasp user interface that promotes high usability with a minimal learning curve. Across all of the supported platforms, the app's UI design and structure is maintained for consistency.

PROVIDES TWO VARIATIONS FOR EASY DISTRIBUTION

The solution provides two variations on each Android and iOS platforms for easy distribution:

HipLink Alert App: This is a basic app version with built in authentication mechanism implemented and allows user to subscribe to HipLink Server to receive Emergency broadcast alerts only over secure channel.

HipLink App: The Advanced version offers complete functionality that includes both receiving and sending alerts, conversations, VoIP calls, contact list access, custom actions, message templates, and more.

The two variations allow enterprises and businesses to manage their license costs as per their needs.

APP DISTRIBUTION WITHIN ENTERPRISE DOMAIN

HipLink Mobile can be easily distributed using third party MDM (Mobile Device Management) solutions and mobile app stores. The apps are tested to work with popular MDM solutions like Toggle, MobileIron and AirWatch.

PROVIDES EASY MANAGEMENT & CONTROL OF MOBILE APP, ITS AUTHORIZATIONS AND ACCESS PERMISSIONS

The solution provides an admin panel on the server through which an admin can control every connected mobile device and its access to information. A general policy can be set for all devices that controls access to features and default usage options. Similarly, specific rules for individual devices can be defined and applied instantaneously as exceptions to the general policy. Communication via mobile devices can be audited via administrator reports. All data in the mobile app can also be wiped out remotely.

END-TO-END SECURITY, CONTENT PROTECTION, & CONTENT CONTROL

The HipLink Mobile app provides end-to-end security using the industry standard cryptographic algorithms such as AES (Advanced Encryption Standard using the Rijndael cipher). Below are aspects that define end-to-end security.

1. All communication between the HipLink server and the HipLink Mobile apps is secure.
2. All the messages and its attachments on the devices are stored in a dedicated, encrypted container within the application
3. All the messages on the devices can be managed with automatic deletion, message expiration, and remote administration.

To ensure message confidentiality, integrity, and authenticity along with security against various attacks HipLink uses the best possible defense mechanism by utilizing Transport Layer Security (TLS). TLS is recognized as a security standard in the enterprise community. TLS, the successor to SSL, offers a robust security protocol meeting IETF (Internet Engineering Task Force) standards for connection security. Using TLS, the HipLink Mobile app supports a wide variety of bit-rate encryption options that include 128, 196 and 256-bit AES encryption configurable by the administrator.

The app makes use of a process called “single session handshake”. By using this process, the TLS encryption key is constantly changing on each communication session between the HipLink server and the mobile device. This enhances the security of the app and reduces the risk of a breach or information compromise.

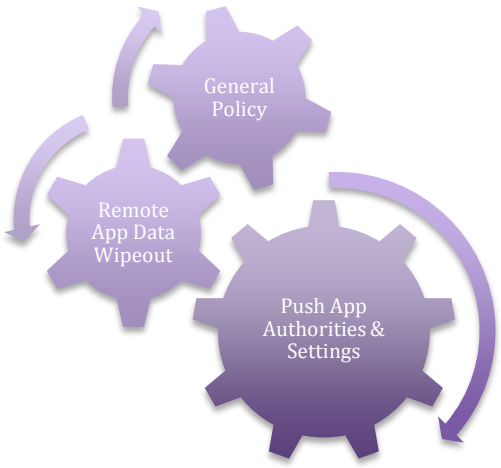
HipLink Mobile offers a short Time to Live (TTL) mechanism for data communication. This reduces life span of data communicated to the mobile devices and enhances security standards.

Security features apply to all phases of message delivery. This is for both messages sent to the phone and responses back.

APP REMOTE ADMINISTRATION, ACCESS CONTROL & GENERAL POLICY

One of the most essential aspects of the BYOD model is to remotely manage and control the data inside the employee (mobile consumer) devices. HipLink Mobile allows corporate administrators to have complete control over company data on employee devices in a manner that does not affect or intrude into their personal information.

The following actions are available to administrators from the HipLink server:



1. Push and enforce application settings remotely from a HipLink server to the device.
2. Push application capabilities and permissions remotely from a HipLink server to the device.
3. Delete all or selected data, including file attachments, stored in the device application.
4. Lock out access to a HipLink server and other HipLink users.
5. Define a general policy for general authorities and application settings applied to all devices.

Enables Enhanced Messaging Workflows for Every Day Operations

The HipLink Mobile app supports several advanced workflows that are required by modern day organizations for successful operational functionality. Besides the simple secure chatting workflow, the solution also provides support for the following:

1. 2-way communication with canned response choices
2. Automatic escalations – sending messages to backup individuals if responses are not received
3. Confidential messaging
4. Broadcast messaging
5. On-Duty messaging – cross checking work schedules and sending messages only to those who are on duty

HipLink Mobile users can also carry out the following actions:

- Browse contact directory stored in the HipLink server and save contacts to the local favorites list.
- Confirm or reject a received alert to let the sender know about their availability / intention toward a request.
- Respond to an alert with a custom response.
- Forward alerts to other users.
- Send and receive file attachments with alerts and chats to share images, audios, video, and files.
- Send and receive their GPS location with alerts for easy tracking.
- Send offline messages to users that are not available.
- Update their group subscriptions
- Make or Receive Audio/Video Internet calls (depend on third party service)

- Ability to recall sent alerts

READY FOR HIPAA COMPLIANCE

HipLink Mobile is Health Insurance Portability and Accountability Act (HIPAA) compliant and due to HIPAA requirements provides:

- Confidential data (e.g. PHI) protection in activity logs and audit trails.
- End-to-end secure communication between HipLink servers and mobile apps with AES encryption algorithm using TLS.
- Device level data protection with the AES encryption algorithm (using 256 or other bit keys) to protect messages and received media content.
- Use of server side enforcement for allowing confidential data to be sent to only secure users and prevent messaging of secure information to insecure users.
- Mobile app security to prevent access of information (messages and media content) by unauthorized personal.
- Remote administration to manage and control mobile app access.
- Ability to remove (all or selected) data on a device from remote admin console.
- Ability to disable mobile app from remote admin console.

REAL-TIME MESSAGING WITH PUSH NOTIFICATION SUPPORT

HipLink Mobile app supports messaging in real time where messages can be received within seconds after being dispatched. All the messaging workflows are designed to be 100% deterministic, letting the dispatcher know immediately if the message delivery has succeeded, failed, or if a message has been put on hold for later delivery. In the case of later delivery, the messages are sent when the recipient comes online.

PUSH NOTIFICATION

Push notifications are used for informing offline users of new messages. Push notifications are used on the Apple and Android platforms.

ALWAYS ONLINE

HipLink Mobile supports an always online status for its mobile users. The intention behind the design is to keep the user online for easy access to new messages sent in real time. The Android app has a special capability to start automatically on device reboots making use of cutting edge Android OS system calls. Even though an always online status is supported HipLink Mobile is designed to run efficiently in the background and exert the least amount of pressure on device battery drain. The iPhone app is tested to perform at an average battery drain of approximately 2% per hour whereas the Android app drains approximately 3% per hour during normal device operations. The impact on the battery can be affected by individual device preferences and the overall age and health of the battery.

Audit Trail and Full Traceability for All Communication

The HipLink server provides a full audit trail for all server-to-device and device-to-device communications. Any message can be traced and its dispatch status can be tracked from a single easy to follow reports panel. The HipLink Mobile app provides detailed reporting for each message which includes:

1. Delivery report on message received at the mobile device.
2. Message read report which shows when the user actually reads a message.
3. Message confirmation, rejection, or custom 2 way response status for instances where the receiver sends his choice/response to a message.

When a message first arrives, a delivery receipt is sent back to the sender. Message recipients have the ability to actively acknowledge or ignore the message which is then also transmitted back to the sender. In addition to acknowledgement, message receivers can respond to a message using free-form text or templates. Responses are kept with the original message in system log files for continuity purposes.

Administrators are provided a full audit trail, including the ability to run reports on the timing of message delivery and how quickly read receipts are returned from each user's Smartphone. This supports compliance with corporate security standards by ensuring that all communications are logged for information auditing purposes.

The server also provides detailed activity logs for each of its processes. An administrator can access log entries that show all the workflows and processes working under a HipLink module and can get information about these activities.

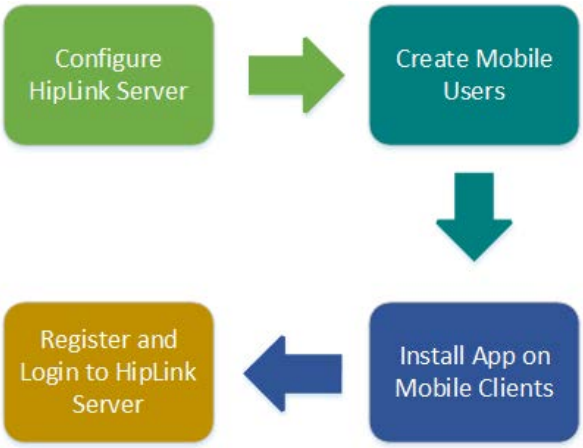
Key Features of HipLink Mobile

- Unified inbox view for chat and alerts
- Separates critical messages from less important ones with various severity levels.
- Secure delivery of messages and responses.
- Automatic delivery of receipts for messages.
- Active acknowledgement of message and free-form text response.
- Directory look-up using contacts search and the ability to mark contacts as favorites.
- User authentication that is LDAP compatible.
- Remote application data wipe and administration.
- Leverages cellular and Wi-Fi networks.
- Supports a variety of devices to accommodate corporate BYOD policies, hospital-employed staff, and independent consultants.
- Real-time messaging for online users, with support for offline messages.
- New message notification alerts for offline users using platform specific push notifications services.
- Personalization of ringtones for message severity levels along with other display settings.
- Persistent alerting for critical and emergency severity messages.
- Multiple format file attachment support.

- One click callback to numbers in the message body.
- One click text to numbers in the message body.
- One click to open URLs embedded in the message body in the device browser.
- Ability to hear messages with text to speech and canned response choices.
- Ability to view and send GPS location coordinates of a user's device with messages.
- Ability to define message expiry.
- Ability to automatically clean message folders by choosing to clear old messages after certain days.

EASY TO DEPLOY IN 4 STEPS...

A four step process is used to set-up the HipLink server and mobile apps. These steps are:



STEP#1: CONFIGURE HIPLINK SERVER

In this step, the admin needs to setup the HipLink Mobile manager, HipLink Mobile carriers, and HipLink Mobile messengers. After this step, the serve will be ready to receive connections from mobile clients and send messages to these clients.

STEP#2: CREATE MOBILE USERS

In this step, mobile users are defined in the HipLink server devices database. Each mobile user can be associated with a HipLink server user to grant extra authorities for advance features.

STEP#3: INSTALL MOBILE CLIENTS

Installing the HipLink Mobile app on mobile devices can be done over-the-air (OTA) using any MDM solution. Or it can be a manual distribution process that involves installing the app binary by asking users to connect their mobile devices to their computers.

STEP#4: REGISTER AND LOGIN TO HIPLINK SERVER

After installation, the app is required to go through a one time registration process with the HipLink server. Once registered and logged in, the user can communicate securely in real time and use HipLink Mobile to its full extent.

STEP#5: [OPTIONAL] CONFIGURING MOBILE CLIENTS

Mobile users can change settings in their app in regards to display configuration, alerting configuration, and security setup. An app master password can be setup as a second layer of security besides screen lock that will protect from unauthorized access.

STEP#6: [OPTIONAL] DEFINING ACCESS PRIVILEGES AND CLIENT SETTINGS

The HipLink server can be configured to define mobile user permissions and app settings. These permissions and settings if defined are enforced on connected mobile apps. Furthermore, the admin can setup a general policy for all mobile users or specific policies for each connected user.

CHANGING YOUR PAGER STRATEGY OVER TIME

Many organizations have decided to replace their pagers with Smartphones since Smartphones offer richer functionality and more computing power. Due to the stronger coverage capabilities of pagers as compared to Smartphones, a lot of hospitals and enterprises still need to use pagers for certain staff members. However, they also need to be able to provide the power of Smartphones to the majority of their staff members. This means

supporting a variety of communication devices for the foreseeable future. It's an approach that has a mixed bag of devices. The benefit of this approach is that some staff members can consolidate devices using Smartphones while others may continue to use pagers. HipLink Mobile enables you to do what makes sense based on your staff and messaging requirements since it does not force you to replace pagers completely. With the power of the HipLink smart phones can communicate with each other and pagers.

WHO WE ARE?

HipLink Software was founded in 1993 with corporate headquarters in the heart of Silicon Valley California. As a stable, profitable, woman-owned business, HipLink continues to demonstrate a high commitment to its customers, while introducing numerous technological innovations. HipLink Software has been the premier provider of software for wireless text and voice communication to global organizations of all sizes for over fifteen years.

The first implementation of HipLink was in 1995 in a major project with Nextel. Since then, HipLink Software has grown to serve hundreds of customer organizations while benefiting millions of users. Successfully deployed across multiple verticals, HipLink is meeting the needs for IT alerting, alarm management, emergency response, mass notification and business continuity. Customers include Wells Fargo, Unisys, Kaiser Permanente, Honeywell, Hewlett Packard, St. John Medical Center, O'Hare International Airport, General Motors Corporation, Cablevision, Government of Alberta Canada, Westchester County, Toronto Police Department and Lockheed Martin to mention a few.