Worker Manual

AuthentiCare® New Mexico Turquoise Care

Table of Contents

1.0 Introduction

AuthentiCare® is an Electronic Visit Verification (EVV) solution that allows states to comply with the 21st Century Cures Act. The AuthentiCare® web-based portal along with two check-in and check-out methods provides electronic visit verification, scheduling, reporting, and billing.

1.1 Overview

This document provides an overview of the two check-in and check-out methods available to Workers, or the individuals providing Services.

- **AuthentiCare® Mobile Application** – The mobile application via the Worker's Mobile Device using the AuthentiCare® 2.0 Mobile Application.
- **Interactive Voice Response (IVR) System** – The Client's phone to call the toll-free IVR at (800) 903-4676.

1.2 Using this Manual

This User Manual is designed to provide the information for how Workers can get started with AuthentiCare®. Each section may also have one of the following icons to highlight valuable information.

Notes: The information is intended to assist and further explain the material. It may include an important tip or hint for using the system.

Caution: The information outlines actions that, if taken in the system, may have an adverse effect.

2.0   Initial Set Up for AuthentiCare® 2.0 Mobile Application

Provider Administrators for the Provider Agency you are employed with will need to enable the Mobile Application from your Worker Entity Setting page within the AuthentiCare® Web Portal. This action MUST be done by the Provider Agency's Provider Administrator as Worker do NOT have access to the Web Portal.

The Provider Administrator will need to:

- Enable Mobile for Worker
- Create Initial Password for Worker
- Enter the Worker's Mobile Phone Number, including area code
- Enter the Device ID of the Worker's personal Mobile Application/phone
- Enter the Office Phone Number

Once all the above information has been entered, it is the responsibility of the Provider Administrator to share your Worker ID and initial password with you for your initial login session. They should also share with you the Environment ID.

2.1   Download the AuthentiCare® 2.0 Application

The AuthentiCare® 2.0 Mobile Application is available to iOS (iPhone) operating systems 13.0 and newer, or Android version 6.0 and newer. To download the Mobile Application , follow the steps below.

1. Search for "AuthentiCare® 2.0" in the Apple App Store or Google Play Store.
2. Install and open the application.
3. Tap **Allow** for the application to access the Mobile Device's location.

> **Note**: The terms and conditions must be accepted prior to the application opening on the Mobile Device.

2.2   Initial Setup for Environment

Once the Mobile Application is installed, initial setup needs to occur. In order for you to use the AuthentiCare® Mobile Application, you will need to confirm with the Provider Administrator they have enabled your Mobile Application use.

When you first open the AuthentiCare® Mobile Application after download, you will see a screen that requires the entry of a Setup Code. The Live Production Environment (used when you are going to perform actual Client care) code is:

| Live/Production |
| --- |
| NMCCPRD |
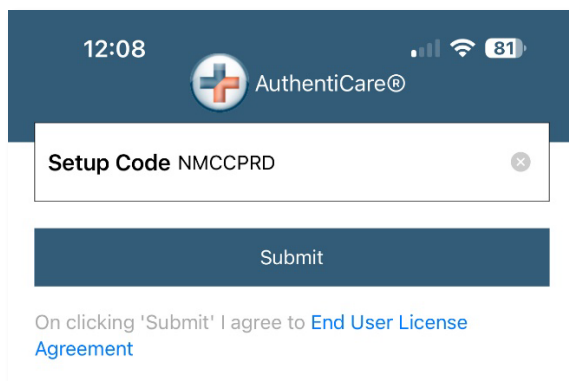
You will:

1. Enter the environment code in the **Setup Code** field.
2. Review the End User License Agreement by tapping **End User License Agreement.**
3. Tap **Submit** which saves the Setup Code and signifies the acceptance of the End User License Agreement.

2.3   Find Device ID from the Settings Menu

After entering the Setup Code, you will be taken to the login screen.

To find the Mobile Application's Device ID:

1. Tap **Settings** on the right side of the screen. The Menu displays.
2. Tap **See Device Identifier** in the Menu. The **Device ID** displays.
3. Tap **OK** to close the window.
4. Assure the Provider Administrator has the correct Device ID. (The Worker can tap to copy the Device ID and then email the Device ID to the Provider.)
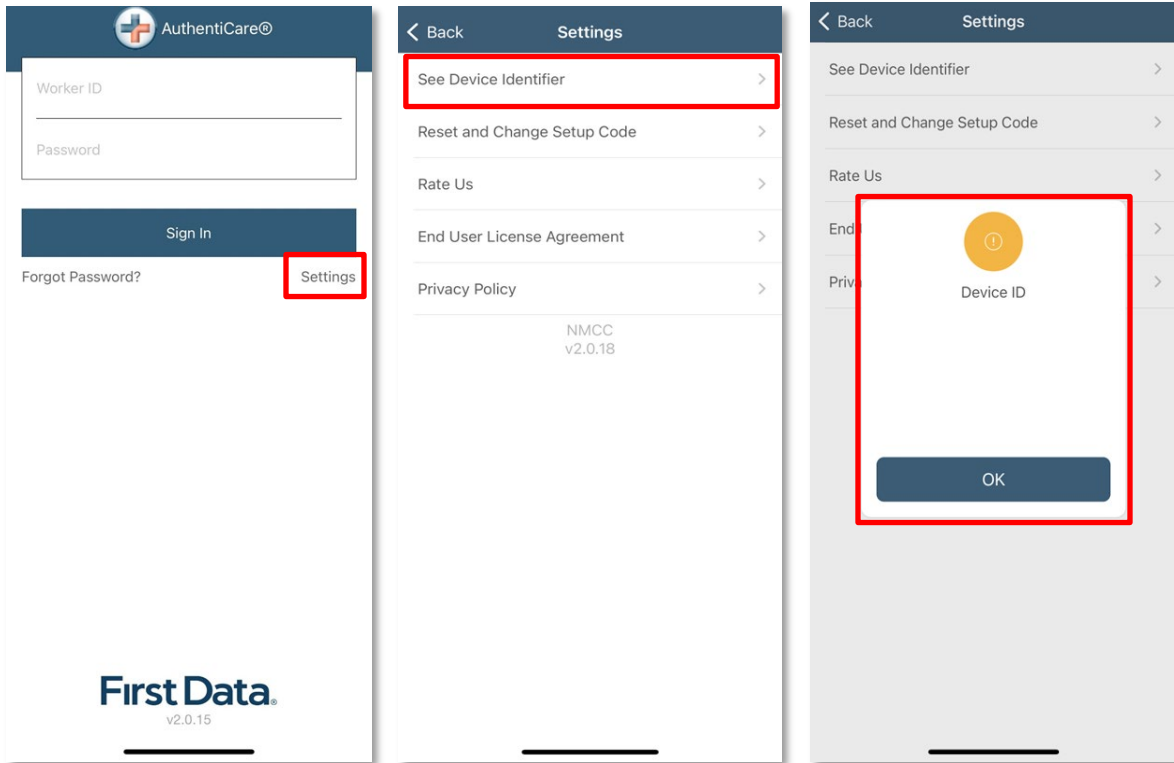
3.0 AuthentiCare® 2.0 Mobile Application

The AuthentiCare® 2.0 Mobile Application can be used to check-in and check-out when service delivery begins and ends.

The following sections outline the process for Mobile Application Setup and Use.

## 3.1 Worker Mobile Application Login – First Use

Once the Mobile Application has been enabled by the Provider Administrator, the Worker can login. Complete the steps below when logging into the AuthentiCare® Mobile Application for the first time.

1. Open the AuthentiCare® 2.0 Mobile Application .

2. Enter your AuthentiCare® Worker ID and temporary password assigned by the Provider Administrator on the *Login* screen. Tap **Sign In**.

> **Note**: Provider Agencies will create the temporary password for Worker on the *Worker Entity Settings* page in the AuthentiCare® Web Portal.

3. You will need to create a new password after logging into the AuthentiCare® 2.0 Mobile Application for the first time. Enter the temporary password in the "Current Password" field, and the new one in the "New Password" and "Confirm New Password" fields.
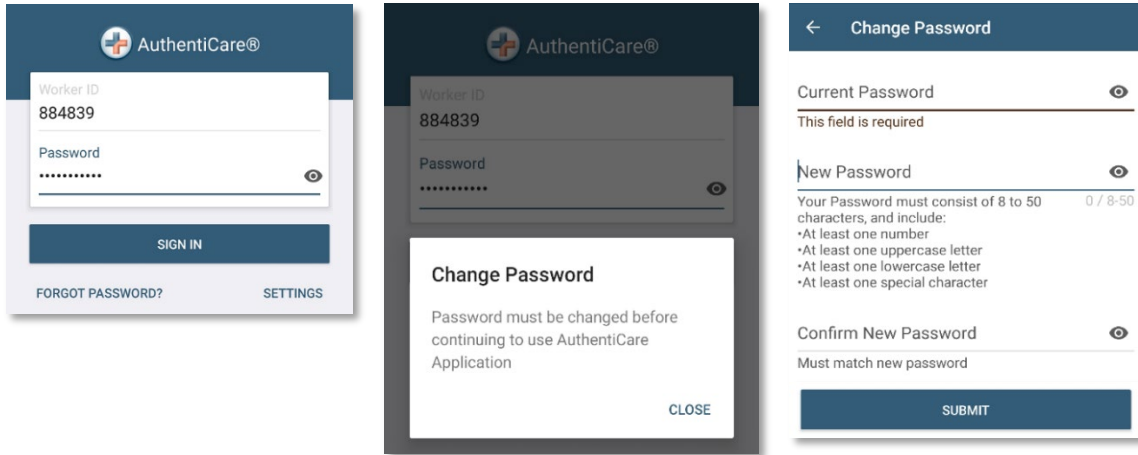
4. Once the password is changed, the screen will go back to the *Login* screen.

5. Enter the **AuthentiCare® Worker ID** and **Password** on the *Login* screen.

6. Tap the [icon] icon which opens the "eye" [icon] to display the password as typed or after the full password is typed. Tap the icon again to cancel the display of the password.

7. Tap **Done** on the keyboard to display the full screen or simply tap **Sign In.**

8. Once the AuthentiCare® Worker ID and password are entered, the session begins.

⚠️ **Caution**: If there are three unsuccessful attempts to log in to the Mobile Application , the account will be locked. You will have to call the Provider Agency to unlock the account. The Provider Agency will create a temporary password and instruct you to enter the new temporary password and then create a new password.

📝 **Note**: You can log in to create a session for the day when and where you have internet access, and then drive to the Client's service location to process a check-in for Client service delivery. Logging in to begin a session is not the same as processing a check-in for Client service delivery.

3.2   Forgot Password

Workers can change their password in AuthentiCare® if an administrator from their Provider Agency has entered their email address on the AuthentiCare® Web Portal (on the *Worker Entity Settings* page). To use the *Forgot Password* feature, complete the steps below.

1. Open the AuthentiCare® Mobile Application .

2. Tap **Forgot Password**.

3. The *Forgot Password* screen displays.
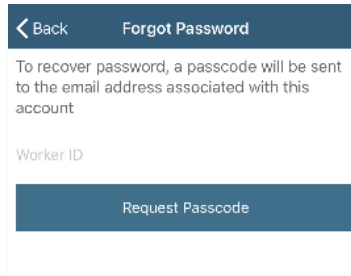
4. Enter your **AuthentiCare® Worker ID**. To recover a password, you must have an email address listed in AuthentiCare® on the *Worker Entity Settings* page in the AuthentiCare® Web Portal; your Provider Agency will have access to the AuthentiCare® Web Portal. A new passcode will be sent to the email address associated with your Worker account in the AuthentiCare® Web Portal.
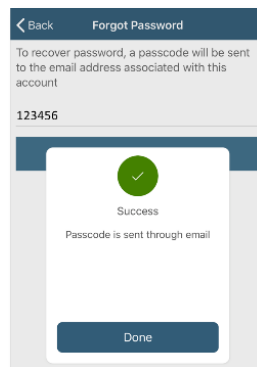

5. Once you receive the passcode in your email, type in the passcode and your new password in the **New Password** field. Confirm the new password by entering the new password in the **Confirm New Password** field too. Then, tap **Submit**. All passwords must follow the secure password rules listed on the screen.
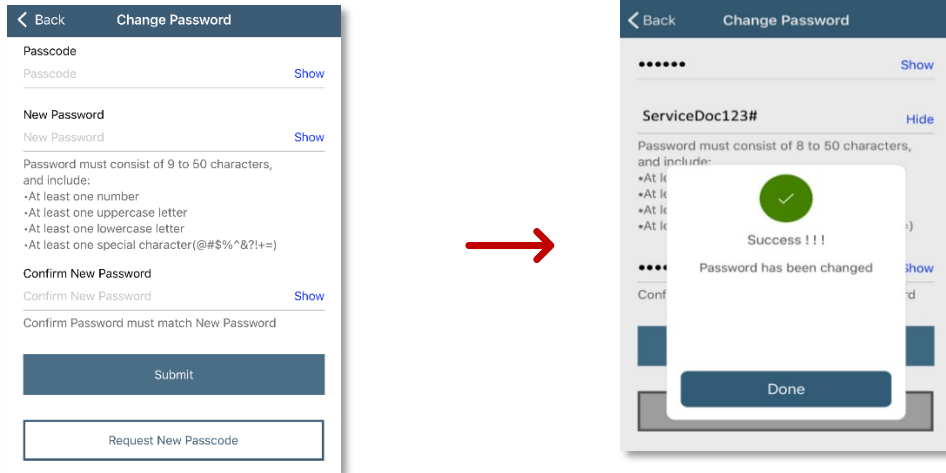
3.2.1   Change Password after Successful Login

To change Mobile Application passwords after successfully logging in, follow the steps below.

1. Tap **Settings** in the lower right corner of the screen.

2. Select **Change Password** to display "Current password," "New password" and "Confirm new password" fields.
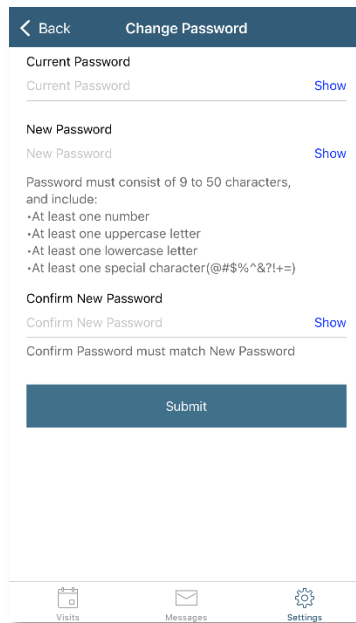
3. Enter the temporary password in the *Current Password* field, and the new one in the *New Password* and *Confirm New Password* fields. Tap **Submit.**

4. When the *Password Change Success* screen displays. Tap **Done**.
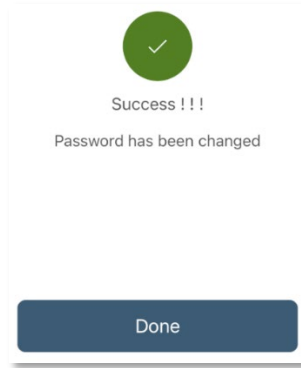
3.3   Access the Calendar

To access the calendar in the Mobile Application , follow the steps below:

1. Log in to the Mobile Application using the Worker ID and Password.
2. Tap the **current date (Today)** at the top of the mobile screen to open the calendar.
3. The calendar defaults to the current date. Tap the calendar date to display any Visits you have already completed for the day plus any pending Visits.
4. Tap any past dates to display any Visits for that date.
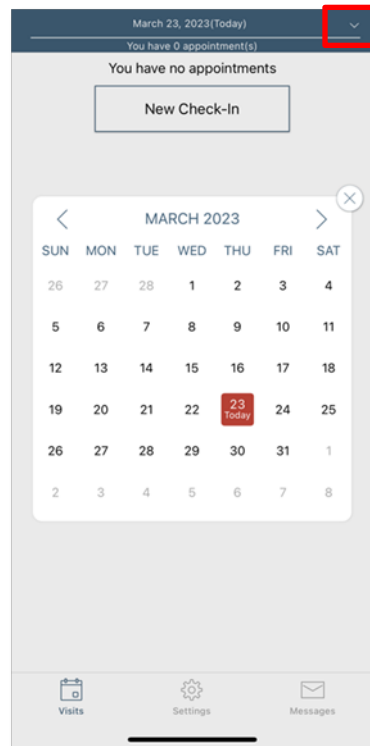
## 3.4   Worker Check-in

Once you arrive at the service delivery location, follow the steps below to check-in.

3.4.1 Checking-in if Scheduling is Not Used

When you arrive at the Client location, you will:

1. Open the AuthentiCare® Mobile Application
2. Input your **Worker ID** and App **Password** to begin the session.
3. Tap **Done** on the keyboard or simply tap **Sign In.**
4. "You have no appointments" displays in the date banner. The Worker will tap **New Check-In.**
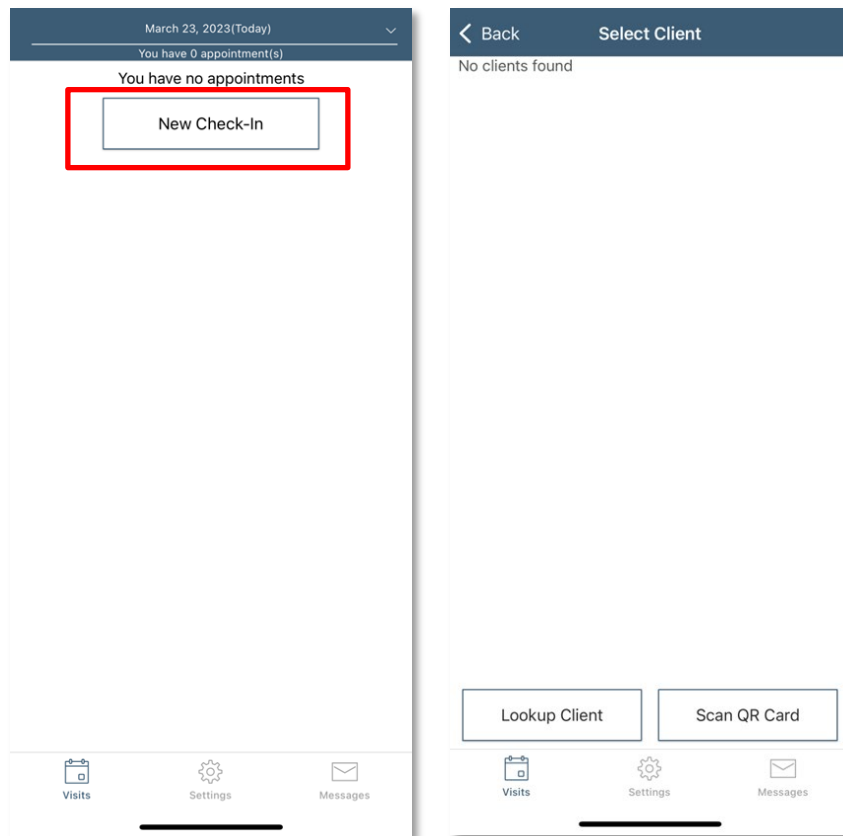
The **Select Client** screen displays with a list of any Clients, associated with the Provider, found near the current location of the Mobile Application.

1. If the Client's name is on the list, tap anywhere in the **Client's name** field.
2. Tapping a Client name leads to the display of the Visits screen.

3.4.2   Lookup Client-Enter the Client's ID Number or Last Name

If the Client's name is not listed on this screen, the screen will display "No Clients found." The Worker will:

1. Tap **New Check-In**
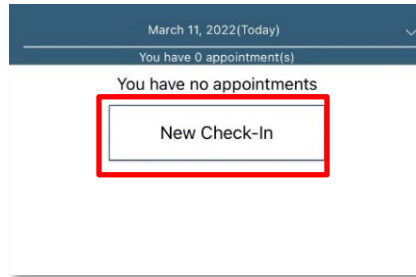
2. Tap **Lookup Client** to open the Lookup Client screen.

3. Input the Client's Last Name.

1. Tap **Lookup**. GPS coordinates from the Check-In process display if the Client lives in a Standard Service Zone.

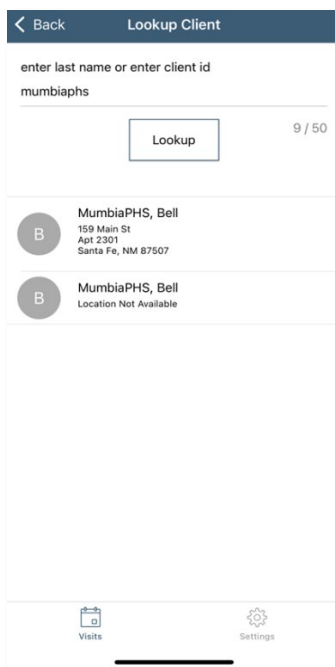**Note**: If you do not have cellular service or internet connectivity at the service location, all screens throughout the check-in and check-out process will display the banner message, "No data connection." You can still log in to the Mobile Application and process a check-in and check-out with this message. To do this, follow the steps in Chapter 2.8.1.

3.4.3 Checking-in if Scheduling is Used

If your Provider Agency uses scheduling, follow the steps below to check in when service delivery begins.

1. Open the Mobile Application .

2. Enter your **Worker ID** in the *Worker ID* field and **Password**.

3. Tap **Sign In**.

4. If your Provider Agency schedules Visits, the visit will appear on the main screen as seen below. To access the calendar to see past or future visits, follow the steps in Section 3.3.

5. If the check-in information looks correct, tap **Submit Check-in**.

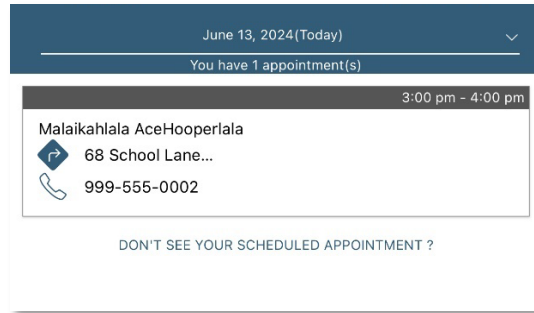6. GPS coordinates and the check-in time from the check-in process will display.
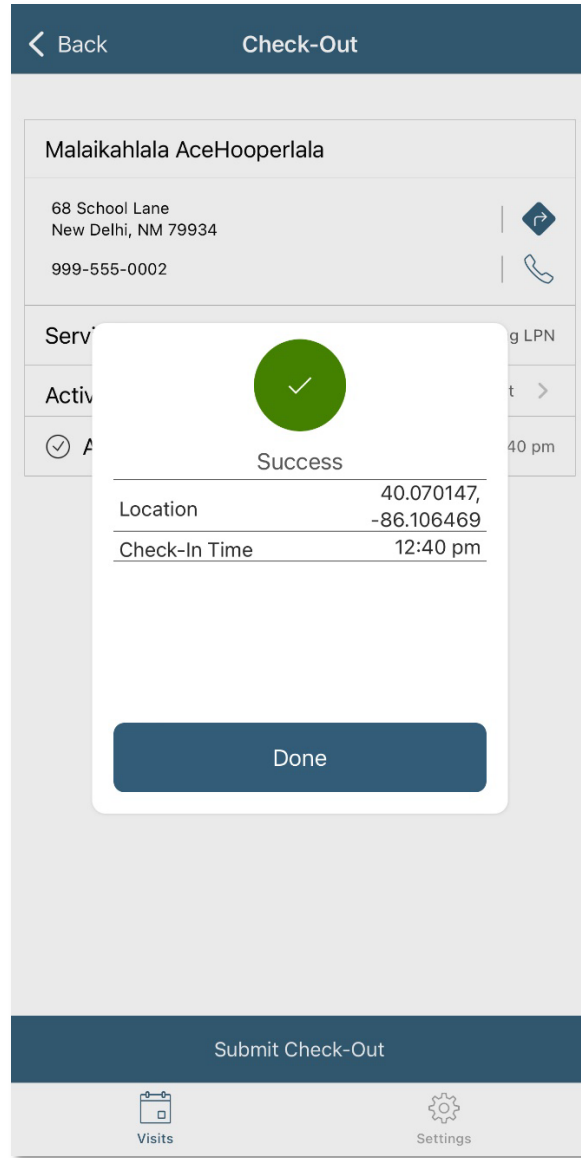
Note: If you do not have cellular service or internet connectivity at the service location, all screens throughout the check-in and check-out process will display the banner message, "No data connection." You can still log in to the Mobile Application and process a check-in and check-out with this message. To do this, follow the steps in Chapter 2.8.1.

3.5   Worker Check-out
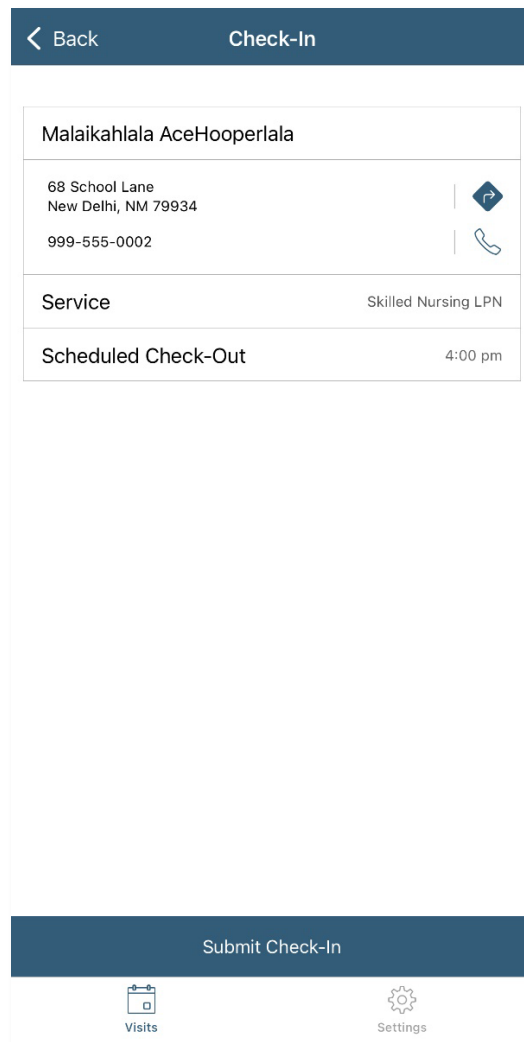
When it is time to check-out of a visit, follow the steps outlined below. This is the same process regardless of your Provider Agency using scheduling.

1. Open the AuthentiCare® Mobile Application .

2. Access visits with pending check-outs on the main screen. Tap on the **In Progress-Pending Check Out** for the visit that needs to be checked out.
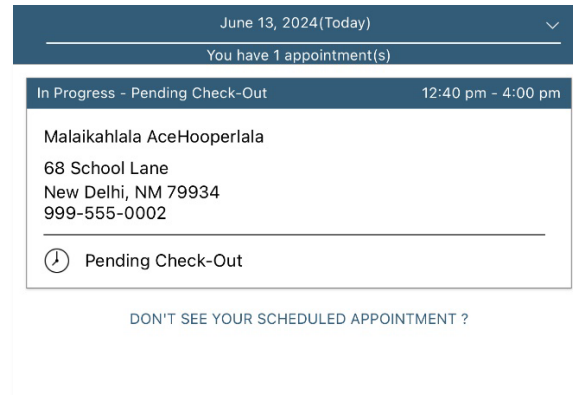
3. The check-out screen displays. If applicable, tap the Activities (tasks) performed during the service delivery. Tap Done once all the activities are selected.
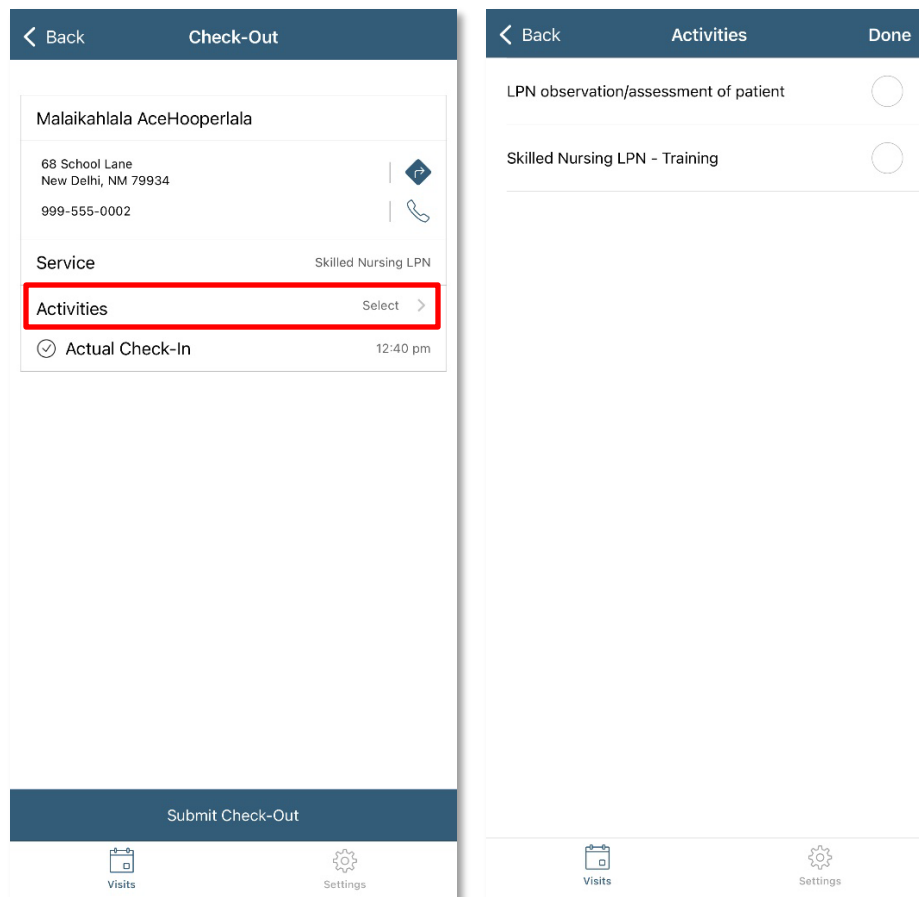
4. Tap **Submit Check-out**.
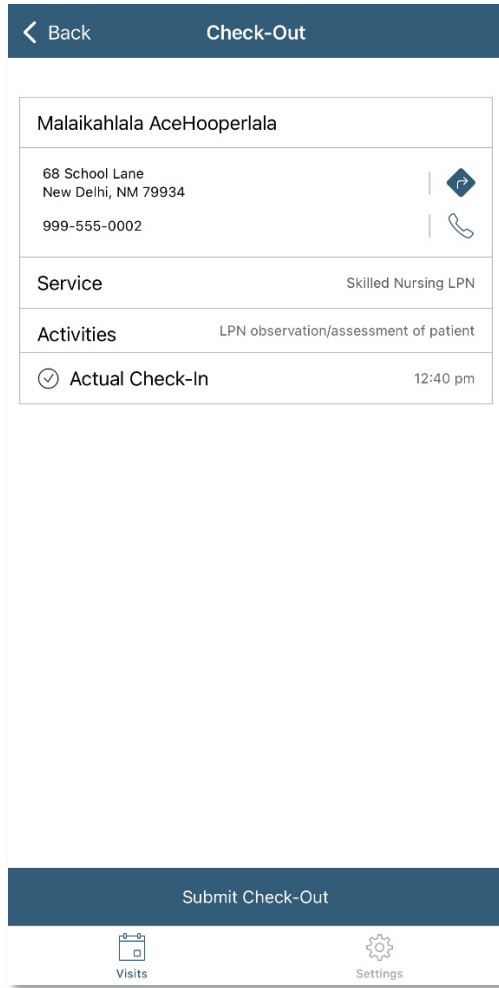
5. The *Check-out Success* screen displays. Tap **Done**.

Document Version: 1.0, Revision Date: 06/13/2024.   16
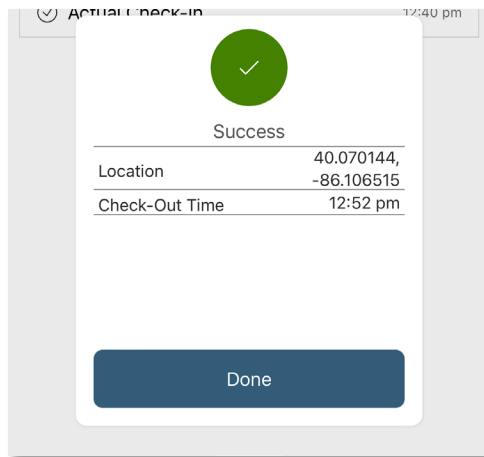
3.6   Service Zones

There are three types of service zones:

- **Standard Service Zone** – There is internet and/or data access. GPS coordinates are captured and used to validate the location of the device during check-in and check-out against the Client's GPS coordinates on record.

- **Limited-Service Zone** – There is no internet or data access. Check in and check out can still occur (including GPS coordinates at check in and check out), but the app shows a message saying "No data connection" in a red banner. The visit will also have a flag showing "Not Synced." More information can be found in section 2.8.1.

- **No Tech Zone** – There is no internet access or cellular service.

3.6.1   Limited-Service Zone

When a Worker is in a Limited-Service Zone, the top of the Mobile Application will display a message in red saying, "No data connection." When there is no data connection, the check-in and the check-out information is stored in the Mobile Application until connection is available. Any visit created when there is no data connection will show a note saying, "Not Synced." When the Mobile Device is returned to an area with service, the "No data connection" message will disappear. Once the application is opened in an area with cellular coverage again, the visit will be sent to the AuthentiCare® Web Portal; the Worker will know the visit was successfully transmitted when the "Not Synced" message disappears. It is recommended that the Worker connects to data or internet the same day the visit was performed to ensure the visit information was successfully synced to the AuthentiCare® Web Portal. If a Worker does not find a data connection by 4:00 AM on the next day, the visit information will not be sent to AuthentiCare®. If that happens, the Worker must contact their Provider Agency administrator requesting a web claim to be entered in the AuthentiCare® Web Portal.
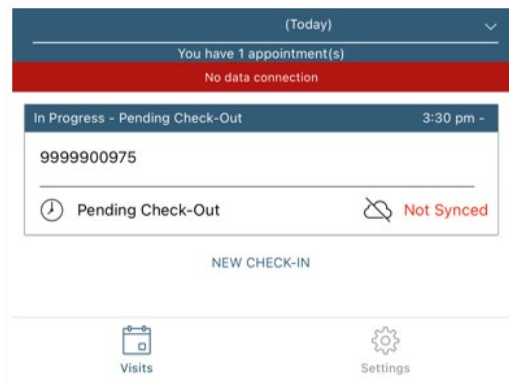
To process a check-in and check-out in a limited-service zone, follow the steps below.

1. Sign into the Mobile Application with your **Worker ID** and **password** in an area with a strong cellular signal or Wi-Fi is available. Do not close the Mobile Application .

2. *If your Provider Agency uses scheduling* – Complete the check-in and check-out process as usual.

    If your Provider Agency does not use scheduling – You will need to manually look up the Client by the Client Medicaid ID and tap **Submit** to start the check-in process. Then, complete the check-in and check-out process as usual.

3. When the visit is complete, it will populate on the *Visits* screen in the Mobile Application . There will be a note that displays "Not Synced." This means that the visit information has not been sent to the AuthentiCare® Web Portal yet.

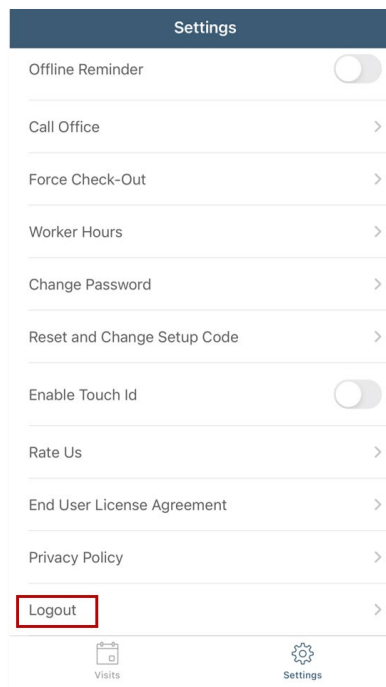4. Once the Mobile Device has cellular signal or Wi-Fi available, the visit information will send to the AuthentiCare® Web Portal and the "Not Synced" message will go away.

3.7   Log Out of the Mobile Application

To log out of the AuthentiCare® Mobile Application , complete the steps below:

1. Tap **Settings** on the bottom right of the screen.

2. Tap **Logout**.

4.0 Using the AuthentiCare® Interactive Voice Response (IVR)

The IVR is designed to capture the information required to create a Claim for the Service being provided. The IVR is available in English and Spanish.

If the phone number you use for the call matches the number for the Client as recorded in AuthentiCare®, then the Client's name will be read by the IVR. If the system does not recognize the number, then you will be asked to enter the Client's ID number.

If your language preference is Spanish, the Provider Administrator will need to update the language in the Language Preference field on the *Worker Entity Settings* page.

> **Note:** When checking out, if the IVR reads more than one name, which means you have not checked out for previous Claim(s) for which you had checked in. In order to resolve this, the Claim(s) must be completed on the AuthentiCare® Web Portal with the appropriate check out times.

The IVR then reads the list of Services that you could potentially be providing for this Client. For consistency, the Services for a specific Client are read in the same order on all calls. This same list also applies during check out calls. Additionally, during check out you must specify activities (tasks) completed during the Visit if the Services provided required activity codes.

The IVR then reads back all of the information in order for you to verify its accuracy. If there are any errors, you have the option to start over and correct the errors. If the information is correct, then the call is completed, and you are checked in or out depending on the option chosen at the beginning of the call.

If you are there to provide Services for more than one Client, you must check in for the first Client and at the end of the call when given the option to return to the main menu, choose that option and check in for the second Client. You can repeat this process as many times as necessary.

When checking out, you will need to follow the same process – check out for the first Client, return to the main menu as needed to check out for additional Clients.

Each time you return to the main menu on either a check-in or check-out call, the beginning time of the call is reset.

The IVR's phone number is **(800) 944-4141**.

4.1 Workers with More Than One AuthentiCare® Worker ID

Workers who have more than one Worker ID, because they work for more than one Provider, cannot accidently sign in using the ID not matched to the Client. If they try, the IVR will play the

Document Version: 1.0, Revision Date: 06/13/2024.
19

following message "You have entered an incorrect Worker ID. Please enter a different Worker ID followed by the pound sign."

4.2 Using the IVR from an Unauthorized Phone Number

The system will not prevent you from performing a check-in or a check-out from a non-verified phone number.

> **Note**: If you call the IVR using a phone number not listed on the *Client Entity Settings* page in the AuthentiCare® Web Portal, a critical exception will populate on the claim.

If you are calling from an unauthorized phone number, you will hear the phrase, "You are calling from an unauthorized phone number." The IVR will allow check-in and check-out, but the visit will be flagged with a critical exception on the Claim.

5.0 Activity Codes

The table below lists EVV services that allow activity code entry on the IVR system. Although an EVV service might have this feature, using activity codes may be optional. If an EVV service is not listed in the table, selecting activity codes is not available for that particular service.

PCS Service Name	Activity Code (Phrase stated on the IVR)	Activity Code Number
Personal Care – Consumer Delegated (T1019) **Personal Care – Consumer Directed Visit (99509V)**	Hygiene and Grooming	1
	Individual Bowel and Bladder	2
	Meal Preparation and Assistance	3
	Eating	4
	Household Services and Support Services	5
	Supportive Mobility Assistance	6
	Hauling and Heating Water	7
	Support Services	8
EPSDT Personal Care (S5125)	Hygiene / Grooming	10
	Toileting	11
	Meal Preparation	12
	Eating_	13
	Support Services	14
	Mobility Locomotion	15
	Transfers	16
	Dressing	17
	Minor Maintenance of DME	18
	Light Housekeeping	19
	Assistance With Taking Medications	20

Home Health Service Name	Activity Code (Phrase stated on the IVR)	Activity Code Number
Skilled Nursing LPN (G0300)	LPN observation/assessment of patient	21
	Skilled Nursing LPN – Training	22
Skilled Nursing RN (G0299)	RN (only) management of POC	23
	RN observation/assessment of patient	24
	Skilled Nursing RN – Training	25

SDCB Service Name	SDCB Activity Code (Phrase stated on the IVR)	Activity Code Number
SDCB - Self Directed Personal Care (SDCB99509)	Hygiene and Grooming	1
	Individual Bowel and Bladder	2
	Meal Preparation and Assistance	3
	Eating	4
	Household Services and Support Services	5
	Supportive Mobility Assistance	6
	Hauling and Heating Water	7

6.0   Support

For additional assistance, contact your Provider Agency.