11.10.2 Release Notes

Last Modified on 11/08/2024 3:03 pm EST

Estimated Release Date (Beta): 10/13/2024

Estimated Release Date (All) : 11/10/2024

Feature Enhancements:

Release 11.10.2	
Specify a time when discontinuing a medication	Prior to this release, when a medication was discontinued it would remain active until EOD on the discontinue date. A User now has the ability to choose a date AND time on the Orders screen and Medication Plan when discontinuing a medication. This will allow Users to choose a date/time in the future or EOD, with schedules automatically becoming inactive once the date/time has occurred. Users will be unable to discontinue a mediation in the past. Known Issues • An issue was uncovered in how times will be displayed when Treatments are discontinued. The time appears to be off by an hour. This will be addressed in a future release.
eMAR -Highlight Discontinued Medications Yellow Instead of Pink	Discontinued medications in the eMAR now appear highlighted in yellow instead of pink. This change was made to align with Industry standards and to assist with individuals who are color blind.
Two-Factor Authentication (2FA) for Positive ID in eMAR	Your agency can now require that Two Factor Authentication (2FA) be performed before a user can access the eMAR. To enable this feature, select SYSTEM SETUP (SUPPLEMENTAL)->eMAR Configuration->eMAR Access requires Two Factor Authentication (2FA) and turn the toggle ON Users must then set up 2FA once in their account by going to ACCOUNT SETTINGS on the Main Menu and scrolling down to the TWO-FACTOR AUTHENTICATION section. Here you can use an app like Google Authenticator, Authy, or Microsoft Authenticator to set up 2FA for NextStep. To do the one time setup, open your Authenticator app and use it to scan the QR code that appears in Account Settings. Once the code is accepted, the Authenticator app will provide you with a code that you can enter into the verification field and then click the Verify button to complete the setup. If it's valid, you will get a verified message. Then, each time you open eMAR, you will need to enter your password and a 6-digit code from the 2FA application you set up for NextStep 2FA.
Lockout User after entering 3 wrong password's screens that require a password to proceed.	Administrators may now require a user to be locked out of the system if the user enters 3 consecutive incorrect passwords. To enable this feature, navigate to Main Menu->SYSTEM SETUP (SUPPLEMENTAL), click on the General section and scroll to the PASSWORD EXPIRATION section. Then turn on the Lock user accounts after 3 incorrect password attempts check box. Once enabled, if a user enters a 3rd consecutive incorrect password, they will be locked out of their account. They will not be able to login OR reset their password. To regain access, an administrator needs to select the user in Main Menu->MAINTAIN USERS and unlock their account by unchecking the Locked checkbox and clicking Update User. You could also reset the password after you update the user.