iPatientCare – AssureCare LLC 170.315(d) (13) Multi-Factor Authentication

Version 1.0.0.0

Last updated: September 15, 2022

About Guide

Revision History

Version	Date	Comment
1.0.0.0	September 15, 2022	Original Document

Conventions

Before using this document, it is important to understand the typographical conventions used to identify and describe information.

Description	Appearance
Field Names, Keys you press and Buttons/Icons you click is shown in Open Sans Semibold.	e.g., Press **Enter**. e.g., Click **Ok** to continue. e.g., Select **Provider** from the drop-down list.
Dialog Box and Application Window Titles are shown in Open Sans italics.	e.g., The *Preview* popup appears.
Cross-References to section and hyperlink are shown in Open Sans Semibold.	e.g., Refer to **Conventions Used** section.
Warning and Alert messages are shown in Italic Quoted Text	e.g., "*Warning and Alert messages*"
Assumption and example are in Italic	e.g., *For example*

Support

You can call, fax or e-mail iPatientCare Support:

Phone: 732.607.2400

E-mail: support@ipatientcare.com

For support, you may also generate a ticket from iPatientCare Support Portal:

http://support.ipatientcare.com

170.315(d) (13) Multi-Factor Authentication

iPatientCare 18.0 supports the following use cases for Multi-Factor Authentication:

1. *EPCS for e-Prescribing of Controlled Substances*: The DEA requires a 2-Factor Authentication sign off for EPCS, meaning when a prescriber electronically sends a controlled substance prescription they must sign it using something they know (e.g. a password) and something they have (e.g. a token). Each prescriber who wishes to e-Prescribe controlled substances must go through an identity proofing and authentication process in order to receive a token. iPatientCare EPCS supports both hardware token (which is a small Key Fob token) and software token using third party app Symantec VIP Access on smartphone.
2. *2FA using Google Authenticator for login*: This is an optional feature available upon request. When this feature is enabled, in addition to the username and password, the user is required to enter a one-time password generated by the Google Authenticator app on their smartphone.
   - Google Authenticator is a software-based authenticator by Google that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP; specified in RFC 6238) and HMAC-based One-time Password algorithm (HOTP; specified in RFC 4226), for authenticating users of software applications.
   - To use Authenticator, the app is first installed on a smartphone and set up with the iPatientCare EHR. The first time a user logs in to iPatientCare EHR, iPatientCare EHR provides a shared secret key in the form of the QR Code, that can be scanned in the Authenticator app or can be manually entered. This secret key will be used for all future logins to the site.
   - To log into iPatientCare EHR, the user provides a username and password. The EHR then computes (but does not display) the required six-digit one-time password and asks the user to enter it. The user runs the Authenticator app, which independently computes and displays the same password, which the user types in, authenticating their identity.
   - With this kind of two-factor authentication, mere knowledge of username and password is insufficient to break into a user's account - the attacker also needs knowledge of the shared secret key, or physical access to the device running the Authenticator app.