User Guide

Contents
User Guide .................................................................................................................................... 1
Overview ....................................................................................................................................... 2
Accessing the HIE Portal ................................................................................................................ 2
   Access ................................................................................................................................................. 2
   Portal Account Set Up ......................................................................................................................... 2
Two Factor Authentication (2FA) .................................................................................................. 3
   Authy & Other Authenticator Applications ......................................................................................... 3
   Security Key (FIDO2) ........................................................................................................................... 5
   Reset Phone Number or Security Key ................................................................................................. 6
   Suspend 2FA ....................................................................................................................................... 6
HIE Portal Login ............................................................................................................................. 7
   Login via Authy – Push Authentication ............................................................................................... 7
   Login via Authy – TOTP Authentication ............................................................................................. 7
   Login via other Authenticator Apps .................................................................................................... 8
   Login via Security Key (FIDO2) ............................................................................................................ 8
HIE Portal Home Screen .............................................................................................................. 10
   Tool Bar Features .............................................................................................................................. 10
Patient Search ................................................................................................................................ 12
Launching Application ..................................................................................................................... 13
   Patient Attestation ............................................................................................................................ 14
   Tile Customization ............................................................................................................................ 15
Applications ...................................................................................................................................... 15
   Application Table ............................................................................................................................. 16
HIE Support & Portal URLs .......................................................................................................... 16
Overview

The Health Information Exchange (HIE) Portal was developed in partnership with hMetrix to provide a superior user experience while leveraging HIE applications. Users with access to clinical data can patient search directly from the home page and launch searched patient data into various applications seamlessly.

All users HIE Portal accounts are protected by secure application or token based two factor authentication.

This user guide explains how to utilize features of the HIE Portal and how to access applications through the site.

Accessing the HIE Portal

To access the HIE Portal, users must:

- Navigate to the HIE Portal URL of their associated HIE. See this section for HIE URLs & Support Contacts
- Log into the HIE Portal with their username, password, and two-factor authentication credentials.

Access

To gain access to the HIE Portal, your organization must have a permitted participation agreement with an associated HIE. A HIE Admin at your organization must request or permission user access via a credentialing tool. If you are unsure if your organization has a participation agreement or you do not know who your HIE Admin is contact HIE Support.

Portal Account Set Up

Users will receive an email with an activation link once their account is created. The email will arrive from ‘donotreply@hmetrix.com’ with the subject line HIE Portal Activation.

Once the user clicks the activation link, they will be required to set up an account password. Passwords are required to be at least 16 characters -with at least one number, one special character, and one capital letter.

After the password is set up, it is time to register two factor authentication.
Two Factor Authentication (2FA)

To improve security, the HIE Portal requires that all users set up two-factor authentication for their portal account. Users have three options to meet the two-factor authentication requirement of the HIE Portal.

1. Twilio Authy Application – the preferred method
2. Other Authentication Applications – such as Google Authenticator, Microsoft Authenticator, Duo
3. Security Key such as a YubiKey

Authy & Other Authenticator Applications

**Step 1.** Users will be presented with a prompt to register for Two-Factor Authentication as shown in the figure below after they set up their password. If the user is not ready to activate 2FA, they may skip activation for the next 5 days. After 5 days the activation of 2FA is mandatory, and the skip button will disappear.

![Register For Two-Factor Authentication](image)

**Step 2.** Select ‘Authy Push or Token’ as the 2FA method from the dropdown list. The alternative of a security key (FIDO2) requires a hardware key. The security key option in discussed later in this guide.

**Step 3.** Users must enter their cellular phone number and click the Register button. When the user clicks the Register button, the HIE Portal will validate that the phone number entered is a cellular phone number. If it is not a cellular phone number, a message will display, and the user will be prompted to enter another cellular phone number. User can click the Ok button and reenter the phone number.

![Registration Failed](image)
**Step 4.** After the phone number has been validated, the Proceed to Activation screen shown in the below figure will be displayed. On clicking Proceed, an Authy account will be created with the given phone number, and the user will be taken a screen to ‘Activate 2FA’. If the user clicks the ‘Cancel’ button a message will be displayed and will be returned to the 2FA Activation screen.

![Proceed to Activation](image)

**Step 5.** Authy will send an SMS text message like the one shown to the right. Authy will autodetect the device type and redirect the user to the appropriate app store to download link. Clicking the link within the text message will prompt the user to download the Authy application onto your registered device.

![Reenter Phone Number](image)

**Step 6.** Use of Authy app is strongly preferred. Users can also use an alternative authenticator app, such as Google Authenticator or Microsoft Authenticator. The alternative authenticator app can be used by scanning the QR code in below figure. Please follow the instructions from the alternative authenticator app to scan the QR code. To activate 2FA, users need to enter a 6-digit token in the Activate 2FA screen from Authy or their alternative application of choice. This 6-digit token is available on the newly added HIE Portal tab in the Authy app or the alternative authenticator app. Users need to enter the 6-digit token in the textbox and clicking the Activate button. If the token is valid users will be granted access to the HIE Portal. Otherwise, users need to reenter a valid token. If the user refreshes or closes the browser tab before activation is complete, the process must start over from the Registration screen.
Security Key (FIDO2)

The security key method of two-factor authentication is the most secure. It requires a hardware or software key that conforms to the FIDO2 standard. Examples are YubiKey, Google Titan, and Feitian ePass FIDO2 security keys. The instructions below assume possession of such a key and have configured a pin on the key. Please note that a security key cannot be copied or duplicated. Backups of the key are not possible. The key is unique and cannot be substituted with another key.

**Step 1.** Users will be presented with a prompt to register for Two-Factor Authentication as shown in the figure below after they set up their password. If the user is not ready to activate 2FA, they may skip activation for the next 5 days. After 5 days the activation of 2FA is mandatory, and the skip button will disappear.

**Step 2.** Select 2FA method as ‘Security Key (FIDO2)’ from the dropdown list.

**Step 3.** Insert the security key into the USB port and click the register button to register the key with the HIE Portal.

**Step 4.** Users will be presented with a security screen like the one below. Users need to enter the pin and click OK to continue. Please note that the screen depends on the operating system in use.

**Step 5.** Users will be prompted to touch the security key’s button or biometric scanner. Once touched, the key will be registered against the user’s HIE Portal account and the screen will be redirected to the HIE Portal. If the user refreshes or closes the browser tab before activation is complete, the process must start over from the Registration screen.
Reset Phone Number or Security Key

If you need to reset your phone number or security key, you may click on the ‘Request phone number reset’ or ‘Request key reset’ link in the HIE Portal 2FA screen. An email will be sent to the HIE Support staff requesting a Support team member to approve or deny the request. A support team member will verify your identity to approve the request is legitimate. If approved, you must repeat the activation process described in Two-Factor Authentication Set Up section above.

Suspend 2FA

If you have forgot or misplace your phone or security key temporarily but require important reporting information from the HIE Portal, you may click on the ‘Forgot your phone? Request help!’ or ‘Forgot your key? Request help!’ link in the HIE Portal 2FA screen. An email will be sent to HIE Support requesting a support team member to approve or deny the request. A support team member will verify your identity to ascertain that the request is legitimate. Once the request is approved, the user will be allowed to login to the HIE Portal without 2FA for a temporary period. Support will monitor these requests closely and has strict protocols in place prevent malicious behavior. Please note this feature is only available during normal office hours.
HIE Portal Login

Once 2FA has been activated, users can log into the HIE Portal with their username, password, and two-factor authentication credentials. All future account login attempts will need to follow the steps described below depending on 2FA method.

Login via Authy – Push Authentication

Step 1. Users who registered the Authy app with the Portal can retrieve pending Push notifications from their phone. All notifications will provide information regarding the request for the user to approve or deny. User should click Deny and contact support if they do not recognize the Push request. Approved requests will grant access to the HIE Portal Home Page. If the notification request is Denied in the Authenticator app, then the HIE Portal will deny the log in, and will redirect to the Login page.

Login via Authy – TOTP Authentication

Authy’s Push notification system requires cellular connectivity. Time-based One-Time Password (TOTP) allows you to authenticate in HIE Portal without cellular connectivity on a phone. Users can generate a TOTP in the Authy application and enter the TOTP token into the HIE Portal instead of the Push approval. The steps below describe the process of user login with TOTP 2FA number.

Step 1. After entering their username and password, users can click to check the option box next to “Trouble receiving an Auth request? Use TOTP Token Instead” on the 2FA screen to use the TOTP token from the Authy app to authenticate.
Step 2. Within the Authy application, users can click the HIE Portal tab to retrieve the TOTP code. The screen will display a token that changes every 30 seconds as shown below.

Step 3. Enter the TOTP token and click Verify to enter the HIE Portal.

Login via other Authenticator Apps

Users using an alternative authenticator app such as Google or Microsoft Authenticator need to follow the steps described below. A Time-based One-Time Password (TOTP) allows authentication in HIE Portal without cellular connectivity on a phone in the same way it works for the Authy app.

Step 1. After entering their username and password, user will be redirected to a screen like the one to the right.

Step 2. Generate the 6-digit TOTP token using the registered Authenticator application on your phone.

Step 3. Enter the token and click Verify complete 2FA.

Login via Security Key (FIDO2)

Users using a security key will need to follow the steps described below. Users must use the same key registered with the HIE Portal. No other key will work.
Step 1: After entering their username and password in the HIE Portal, users will be redirected to a security screen like the one below. Please insert the key in the computer's USB port. Users will need to enter their pin and click OK to continue.

![Security Key PIN Screen]

**Step 2.** Users will be prompted to touch the security key's button or biometric scanner. Once the scanner is do so and the key is validated, you will be redirected to the HIE Portal.

**Step 3.** If the user has temporarily forgotten their security key or lost it and would like to replace it, click Cancel to request a suspension of 2FA or a reset key request.

**Step 4.** Canceled requests will be redirected to the screen below. At the bottom of the screen, are the two options for requesting help. The Retry button will redirect you to Step 1 and clicking the Cancel button will redirect you to the login screen. The forgot key button will send a support ticket to our support staff to assist.

![Canceled Request Screen]
HIE Portal Home Screen

The HIE Portal home screen consists of three sections:

1. The first is the top tool bar which contains an application search box, home button, logout button, and a few other features.
2. The second section is where users can search for patients. Information regarding how to conduct a patient search can be found in the Patient Search page of this user guide.
3. The last section at the bottom is called Your Dashboard. Here users will find all the application they have access to. Details on Your Dashboard can be review in the Launching Applications segment of this user guide.

Tool Bar Features

The tool bar of the HIE Portal contains the following features:

1. **Home Button** – User can click the Home Button to navigate back to the HIE Portal Home Screen from an application page.
2. **Logout Button** – Users can click the Logout Button to sign out of the HIE Portal. Once clicked, the page will navigate back to the login screen.
3. **Send Feedback Button** - Opens a feedback forum in another tab which can be used to send secure feedback or questions to HIE Support. Users are required to fill out the following fields before submitting their feedback. A support ticket will be created the support team to work on and reply to the requesting user.

![Feedback Portal](image)

4. **Product Updates** - Opens a pop out window which will display news and notes about HIE services. Typically, new features or releases of applications will be listed here. A notification icon will appear over the Product Updates button when new content has been published to this feature.

![Product Updates Center](image)

5. **Application Search Bar** – User can use this free text field to search for applications within the HIE Portal by name. Please note that if the application requires a patient first before launching it will not appear in the search results until a patient search is made.
Patient Search

Users can search for patients directly from the HIE Portal home screen. Users must enter a first name, last name, and date of birth to render search results. Gender and Social Security Number fields can be added to narrow the selection.

The results of the Patient Search will appear in order of most likely to least likely matches. Each result will contain a match score and match grade. The possible grades include:

1. Certain
2. Probable
3. Possible

This is fake patient data.
Launching Application

Within the Portal, there are applications which require a patient search and other applications that do not. Before making a patient search, the applications which do not require patient context will display within Your Dashboard. Users can launch these by clicking on the desired application’s blue box or tile.

Applications requiring patient context will not appear in Your Dashboard until a patient search is conducted.

Once a Patient Search is completed, users can launch their selected patient’s data within an application by either:

1. Click on the Patient record within the search results table. This action will cause a Selection App pop-up to appear. User can click the four-box icon next to the application name to launch that application.

2. Once a patient search is completed and a patient record as been selected, applications that require a patient search will now appear within Your Dashboard. Users can launch these by clicking on the desired application’s blue box or tile.
All applications will display within the eye frame of the Portal as shown below. Users can navigate to another application by clicking the application title in the side tool bar. User can collapse the application side menu by clicking on the arrow next to Reports & Applications. The Home button at the top will navigate the page back to the Portal home screen.

![Portal Home Screen]

**Patient Attestation**

Users who attempt to launch an application for a patient whom they do not have an active treatment relationship for, (i.e. are not currently active on their organization’s Encounter Notification Service (ENS) Panel) will be presented with the following warning message.

![Patient Attestation Warning]

The user can choose to select Cancel, which will navigate the page back to the home screen. If the user selects Proceed, they will be asked to enter a reason for attesting to the relationship.

![Select a Reason for Attestation]

14
If the patient for whom you are attempting to launch an application has opted out of the HIE, the following message:

This patient has opted-out from having their data shared through the HIE. Only information required by law is available to treating providers. The patient may learn about their rights and opt back in ________

**Tile Customization**

Applications within a user’s dashboard or in the select application menu after a patient search will appear in alphabetical order by application name with one exception. The Clinical Information service, if the user has access to it, will always appear as the first option after a patient search. Users can customize the order of their application tiles by clicking on the Wrench Icon next to Your Dashboard. A Customize Report Categories popup will appear. Users can click on an application title and use the tool buttons to the right to customize the application order. The Up and Down buttons will move the application up or down by one, while the Top and Bottom buttons will move the application to the first or last position.

**Applications**

The table contains some of the HIE services available for use by approved users. The table provides information on the service name of the product or application, and a brief description of the service. Users may or may not have access depending on their organization type, job role, participation agreement, and HIE region. Please reach out to our support staff for questions or clarification.
<table>
<thead>
<tr>
<th>Service</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Information</td>
<td>Clinical Information gives providers the ability to access critical health information and alerts about patients, including medication data, lab results, radiology reports, encounter information and more.</td>
</tr>
<tr>
<td>Consent Tool</td>
<td>Enables users to register consents on behalf of their patients.</td>
</tr>
<tr>
<td>Encounter Notification System (ENS)</td>
<td>Enables users to receive real-time alerts for patient healthcare events (hospital admissions, discharges, etc.). These are most delivered via the ENS PROMPT application.</td>
</tr>
<tr>
<td>Snapshot</td>
<td>Shows users an overview of patient information. Often used for those needing limited PHI access.</td>
</tr>
<tr>
<td>HIE Admin Tool</td>
<td>Allows HIE Administrators to manage their colleagues’ HIE accounts. User account creation, HIE user verification, access to specific HIE Services, and employee turnover can all be handled via the tool.</td>
</tr>
<tr>
<td>Vaccine Tracking Service</td>
<td>Panel based tool to manage and track patient vaccination status</td>
</tr>
<tr>
<td>State PDMP</td>
<td>Access to PDMP depending on the user’s state, which monitors controlled substances dispensed by prescribers.</td>
</tr>
<tr>
<td>Panel Processor</td>
<td>Enables users to upload files to the HIE for ENS, COVID reporting, etc.</td>
</tr>
</tbody>
</table>

**HIE Support & Portal URLs**

<table>
<thead>
<tr>
<th>HIE Region</th>
<th>HIE Name</th>
<th>Support Phone &amp; Email Address</th>
<th>Portal URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD</td>
<td>CRISP</td>
<td>P: 877.952.7477 E: <a href="mailto:support@crisphealth.org">support@crisphealth.org</a></td>
<td><a href="https://portal.crisphealth.org">https://portal.crisphealth.org</a></td>
</tr>
<tr>
<td>DC</td>
<td>CRISP DC</td>
<td>P: 833.580.4646 E: <a href="mailto:support@crisphealth.org">support@crisphealth.org</a></td>
<td><a href="https://portal.crispdc.org">https://portal.crispdc.org</a></td>
</tr>
<tr>
<td>WV</td>
<td>WVHIN</td>
<td>P: 844.468.5755 E: <a href="mailto:wvhinsupport@crisphealth.org">wvhinsupport@crisphealth.org</a></td>
<td><a href="https://portal.wvhin.org">https://portal.wvhin.org</a></td>
</tr>
<tr>
<td>CT</td>
<td>CONNIE</td>
<td>P: 866.987.5514 E: <a href="mailto:help@conniect.org">help@conniect.org</a></td>
<td><a href="https://portal.conniect.org">https://portal.conniect.org</a></td>
</tr>
<tr>
<td>AK</td>
<td>healtheConnect Alaska</td>
<td>P: 907-770-2626 E: <a href="mailto:help@ak-ehealth.org">help@ak-ehealth.org</a></td>
<td><a href="https://hub.healtheconnectak.org">https://hub.healtheconnectak.org</a></td>
</tr>
<tr>
<td>VA</td>
<td>VHI</td>
<td>P: 866-948-0882 E: <a href="mailto:vhisupport@crisphealth.org">vhisupport@crisphealth.org</a></td>
<td><a href="https://portal.vhi.org">https://portal.vhi.org</a></td>
</tr>
</tbody>
</table>