CRISP

Chesapeake Regional Information System for our Patients

CRISP Portal User Guide

Last Updated:

November 5th, 2024

877-952-7477

www.crisphealth.org

10480 Little Patuxent Parkway, Suite 800
Columbia, MD 21044-9997

CRISP Portal User Guide

OVERVIEW **2**

SOURCES OF DATA **2**

ACCESSING THE CRISP PORTAL **2**

- Access 3
- Portal Account Set Up 3

TWO FACTOR AUTHENTICATION **3**

- Authy & Other Authenticator Applications 4
- Security Key (FIDO2) 5
- Reset Phone Number or Security Key 6
- Suspend 2FA 6

CRISP PORTAL LOGIN **7**

- Login via Authy – Push Authentication 7
- Login via Authy – TOTP Authentication 7
- Login via other Authentication Apps 8
- Login via Security Key (FIDO2) 8

CRISP PORTAL HOME SCREEN **9**

- Tool Bar Features 10

PATIENT SEARCH **11**

LAUNCHING APPLICATION **12**

- Patient Attestation 13
- Tile Customization 14
- Applications 14

TECHNICAL USER SUPPORT CONTACT INFORMATION **14**

- Application Table 14

CRISP

Overview

The Chesapeake Regional Information Exchange for our Patients (CRISP) 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' CRISP Portal accounts are protected by secure application or token based two factor authentication.

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

Sources of Data

CRISP receives data from participating healthcare organizations per Maryland state statute.

Data Types Include:

- Admit, discharge, or transfer (ADTs) information, which can include patient demographic, diagnostic, and insurance information
- Patient-specific clinical summary documents, called Continuity of Care Documents (CCDs)
- Radiology images and reports
- Laboratory results
- List of an organization's patients
- Other clinical that include discharge summaries, care notes, and care alerts.

For a current list of the organizations sharing data, and the type of data they are sharing, visit our website. Data also available, but not listed on the website, includes Continuity of Care Documents through National Networks.

Accessing the CRISP Portal

To access the CRISP Portal, users must:

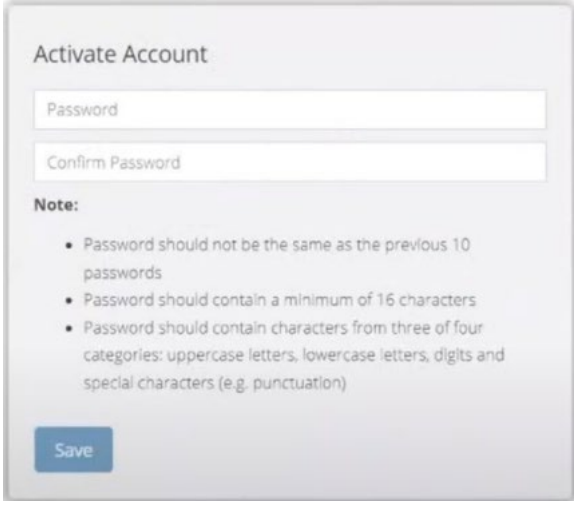
- Navigate to the CRISP Portal URL - https://portal.crisphealth.org
- Log into the CRISP Portal with their username, password, and two-factor authentication credentials.

Access

To gain access to the CRISP Portal, your organization must have a permitted participation agreement with CRISP. 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 Technical User 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 CRISP 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.

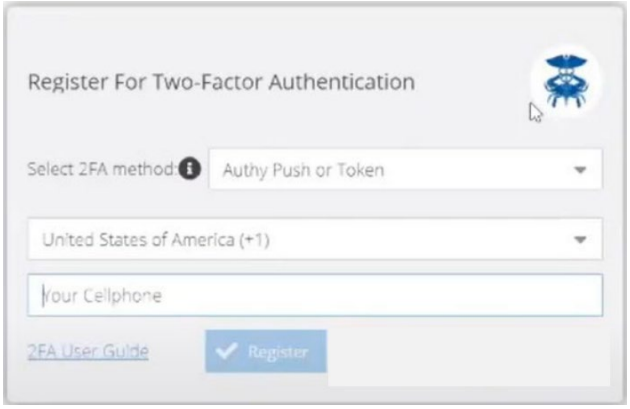
Two Factor Authentication

To improve security, the CRISP 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 CRISP 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

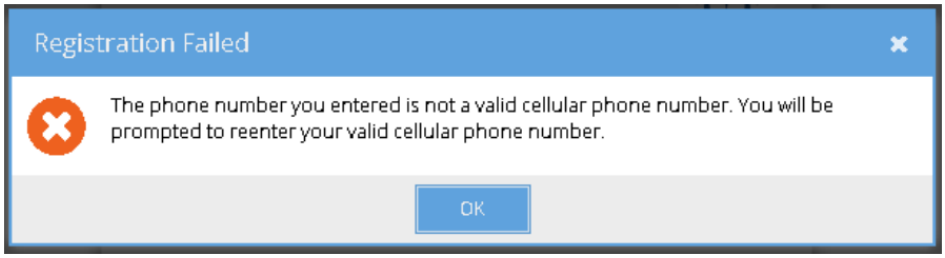
Authy & Other Authenticator Applications

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.

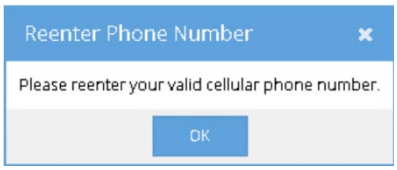


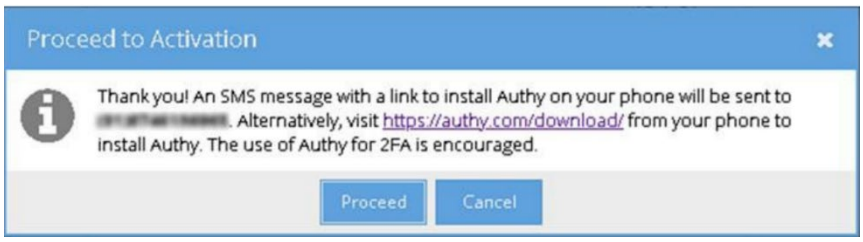
Step 2. Select 'Authy Push or Token' as the 2FA method from the dropdown list. The alternative of a security key (FIDO2) requires a hardware key. The security key option in discussed later in this guide.

Step 3. Users must enter their cellular phone number and click the Register button. When the user clicks the Register button, the CRISP 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.

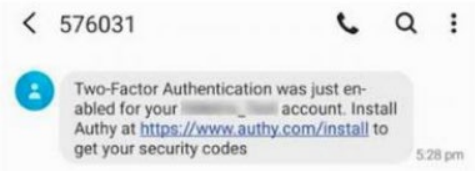


Step 4. After the phone number has been validated, the Proceed to Activation screen shown in the below figure will be displayed. On clicking Proceed, an Authy account will be created with the given phone number, and the user will be taken a screen to 'Activate 2FA'. If the user clicks the 'Cancel' button a message will be displayed and will be returned to the 2FA Activation screen.





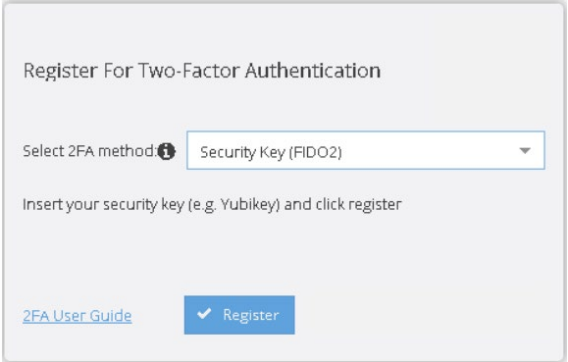
Step 5. Authy will send an SMS text message like the one shown to the right. Authy will autodetect the device type and redirect the user to the appropriate app store to download link. Clicking the link within the text message will prompt the user to download the Authy application onto your registered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



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 CRISP Portal tab in the Authy app or the alternative authenticator app. Users need to enter the 6-digit token in the textbox and click the Activate button. If the token is valid users will be granted access to the CRISP 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 FIFO2 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.

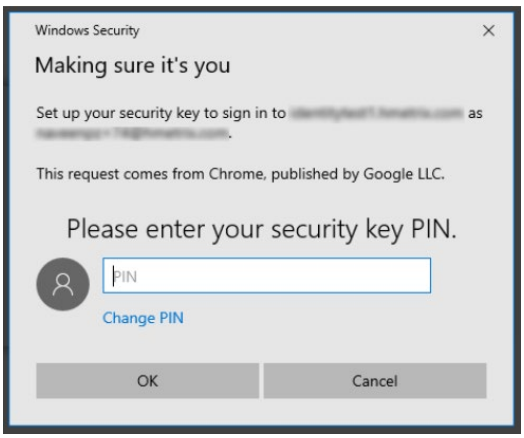


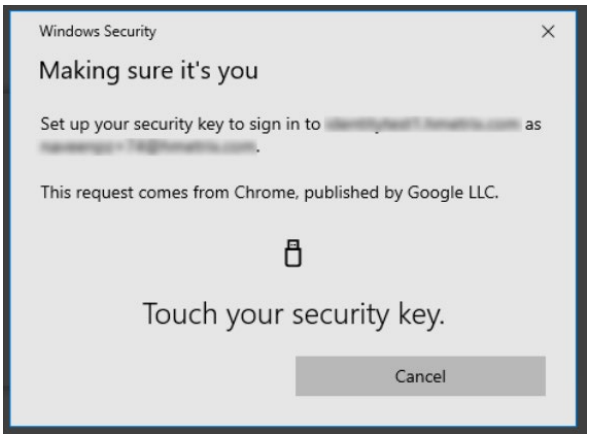
Step 1. Select 2FA method as 'Security Key (FIDO2)' from the dropdown list.

Step 2. Insert the security key into the USB port and click the register button to register the key with the CRISP Portal.

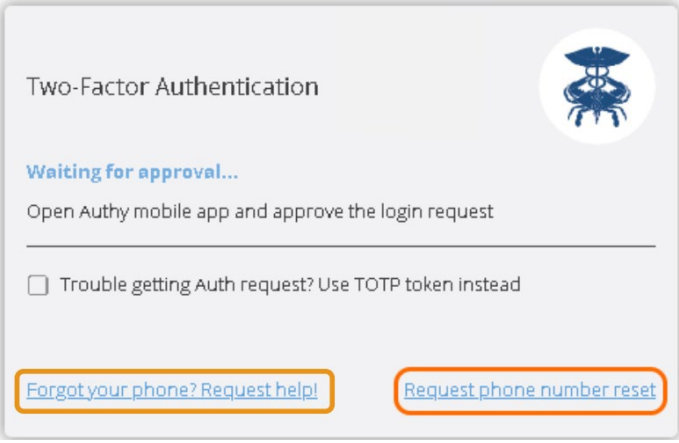
Step 3. Users will be presented with a security screen like the one below. Users need to enter the pin and click OK to continue. Please note that the screen depends on the operating system in use.

Step 4. 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 CRISP Portal account and the screen will be redirected to the CRISP 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 CRISP Portal 2FA screen. An email will be sent to the Technical User 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

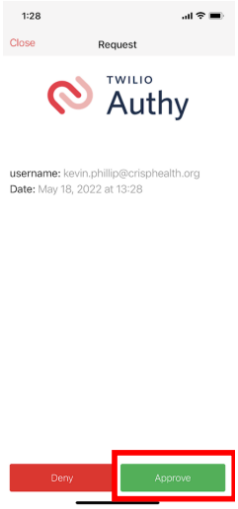
If you have forgot or misplace your phone or security key temporarily but require important reporting information from the CRISP Portal, you may click on the 'Forgot your phone? Request help!' or 'Forgot your key? Request help!' link in the CRISP Portal 2FA screen. An email will be sent to Technical Support User 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 CRISP 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.

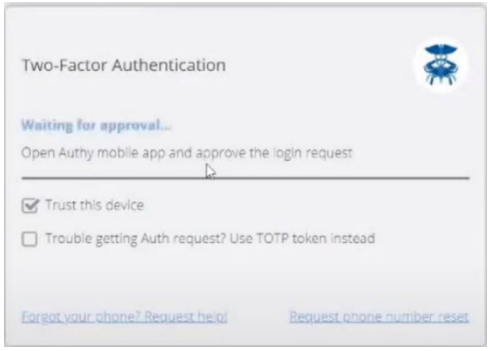
CRISP Portal Login

Once 2FA has been activated, users can log into the CRISP 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

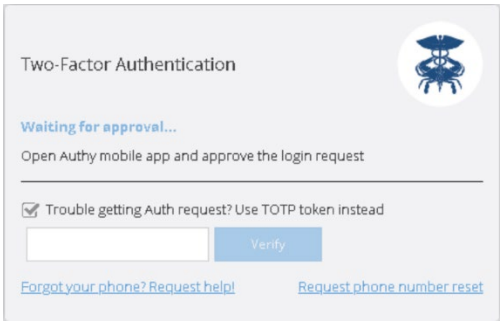
Step 1. Users who registered the Authy app with the Portal can retrieve pending Push notifications from their phone. All notifications will provide information regarding the request for the user to approve or deny. User should click Deny and contact support if they do not recognize the Push request. Approved requests will grant access to the CRISP Portal Home Page. If the notification request is Denied in the Authenticator app, then the CRISP 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 CRISP Portal without cellular connectivity on a phone. Users can generate a TOTP in the Authy application and enter the TOTP token into the CRISP Portal instead of the Push approval. The steps below describe the process of user login with TOTP 2FA number.



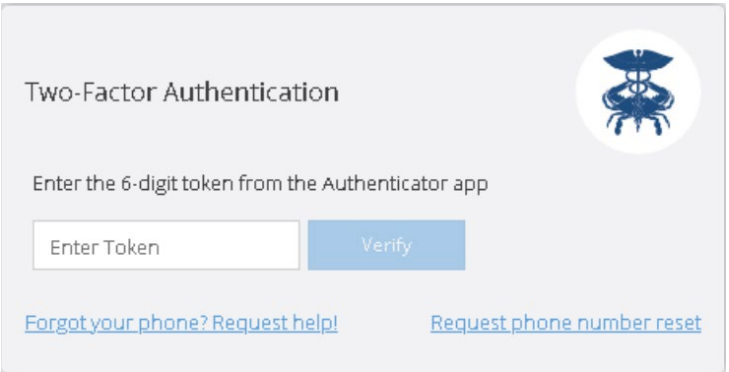
Step 1. After entering their username and password, users can click to check the option box next to 'Trouble receiving an Auth request? Use TOTP Token Instead" on the 2FA screen to use the TOTP token from the Authy app to authenticate.

Step 2. Within the Authy application, users can click the CRISP 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 CRISP Portal.

Login via other Authentication 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 CRISP 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.

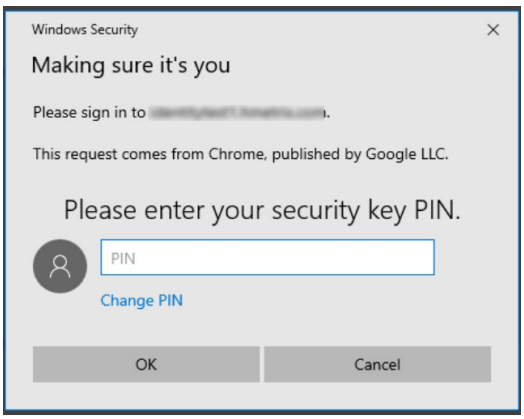
Step 2. Generate the 6-digit TOTP token using the registered Authenticator application on your phone.

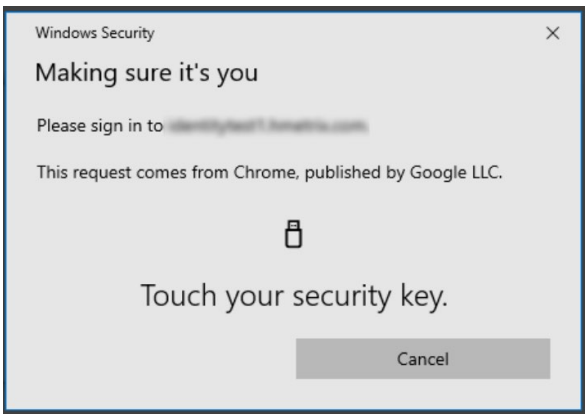
Step 3. Enter the token and click Verify complete 2FA.

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 CRISP Portal. No other key will work.

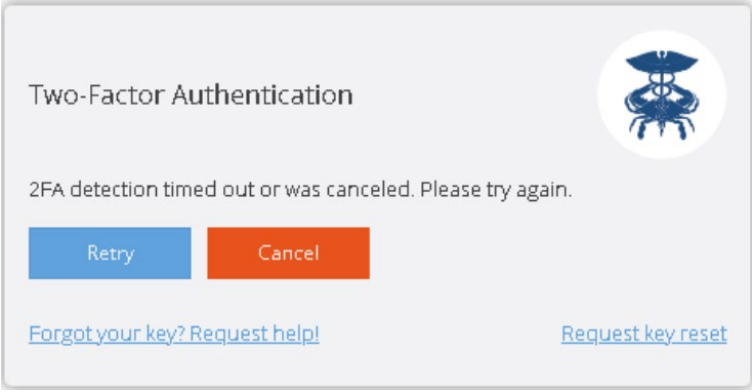
Step 1. After entering their username and password in the CRISP Portal, users will be redirected to a security screen like the one below. Please insert the key in the computers USB port. Users will need to enter their pin and click OK to continue.





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 CRISP 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.

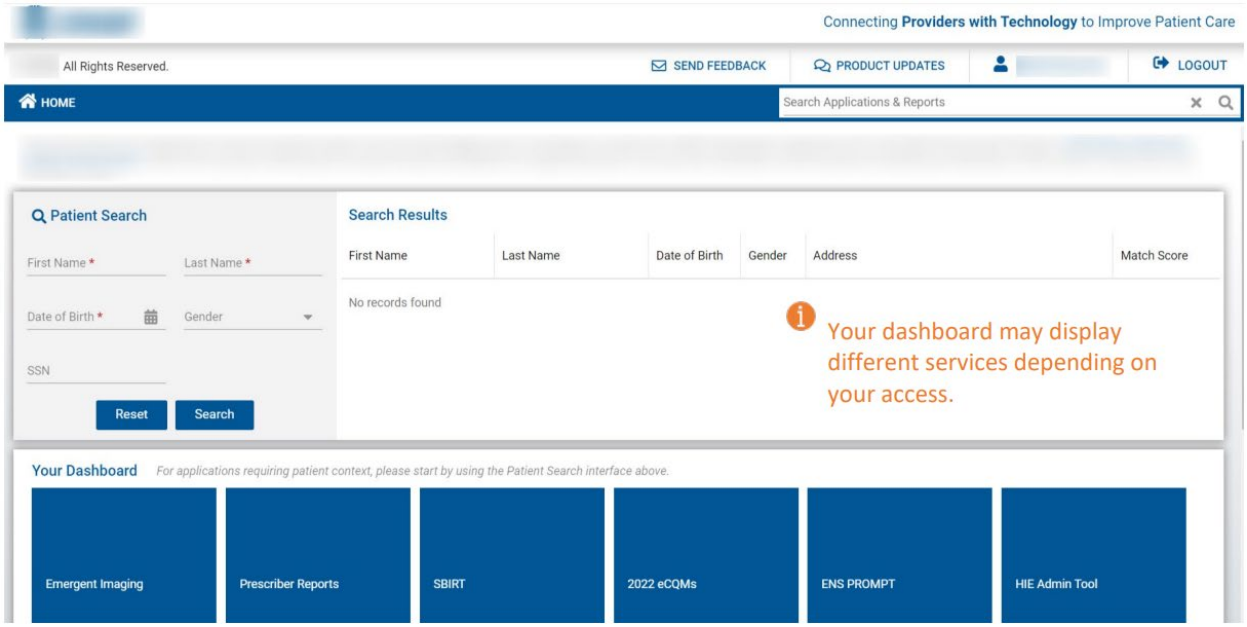


Step 4. Canceled requests will be redirected to the screen below. At the bottom of the screen, are the two options for requesting help. The Retry button will redirect you to Step 1 and clicking the Cancel button will redirect you to the login screen. The forgot key button will send a support ticket to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

CRISP Portal Home Screen

The CRISP 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.

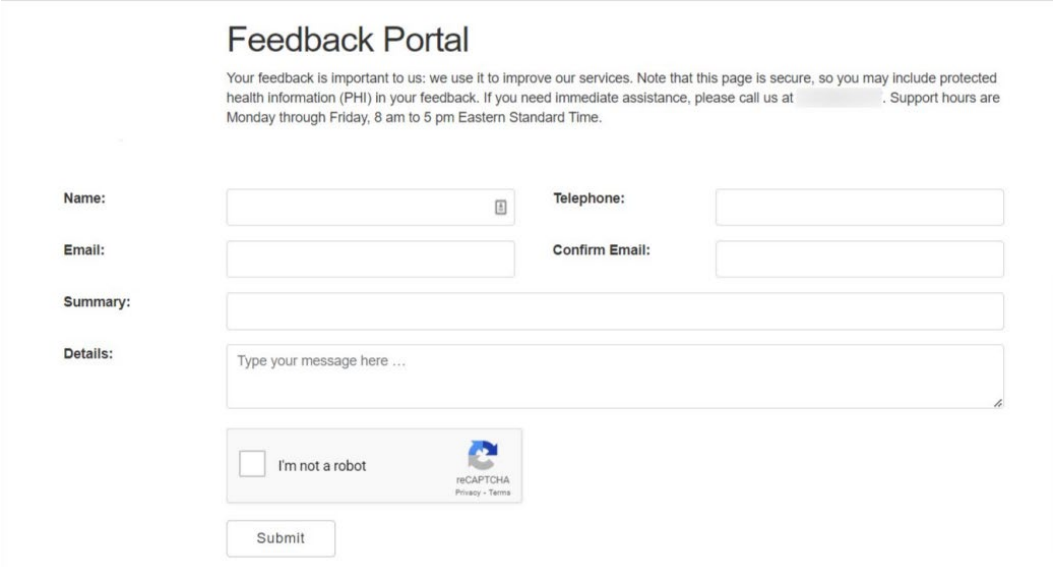


CRISP

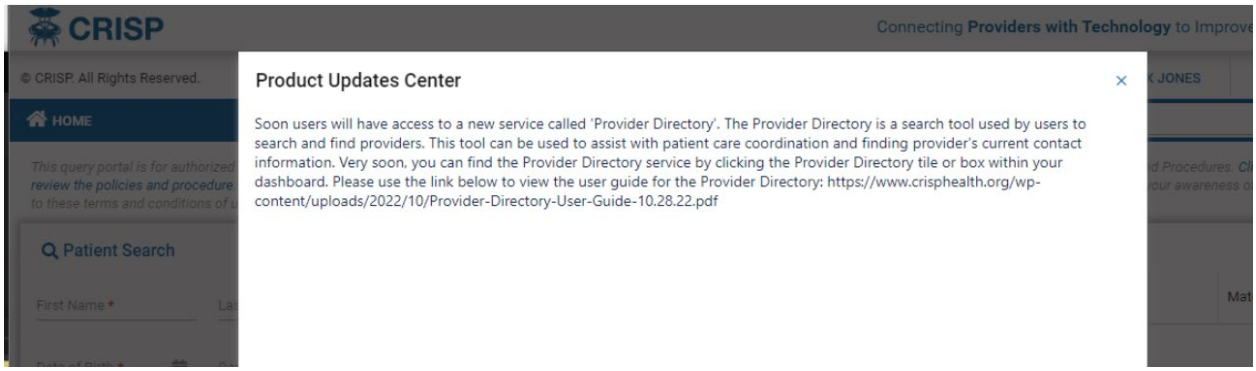
Tool Bar Features

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

1. Home Button – Users can click the Home Button to navigate back to the CRISP Portal Home Screen from an application page.
2. HIE Admin – Users can hover to view the name & email address of their organization's HIE Admin.
3. Logout Button – Users can click the Logout Button to sign out of the CRISP Portal. Once clicked, the page will navigate back to the login screen.
4. Send Feedback Button - Opens a feedback forum in another tab which can be used to send secure feedback or questions to Technical User 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.



5. Product Updates - Opens a pop out window which will display news and notes about CRISP 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.

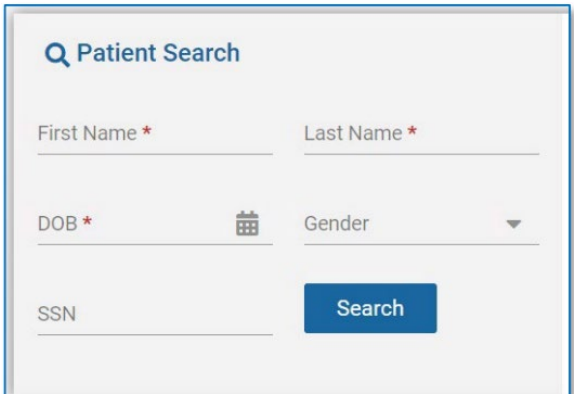


6. Application Search Bar – User can use this free text field to search for applications within the CRISP Portal by name. Please note that if the application requires a patient first before launching it will not appear in the search results until a patient search is made.

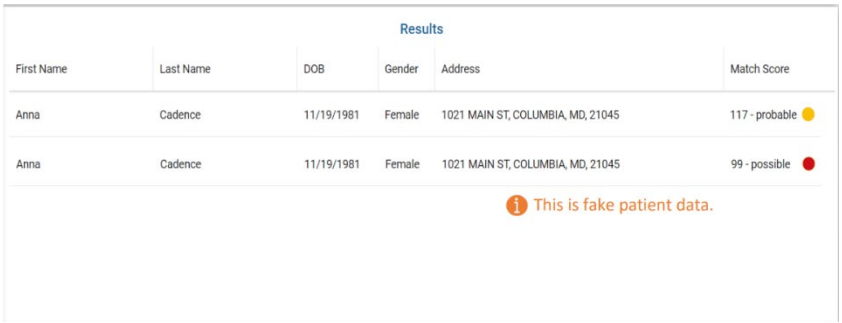
Patient Search

Users can search for patients directly from the CRISP 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. Data entered is not case-sensitive, and dates do not need forward slashes separating the month data and year. Entering 050281 will result in 05/02/1981.

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. Only patients matched using the required fields plus gender and social security number (SSN) will display as 'Certain'. The possible grades include:

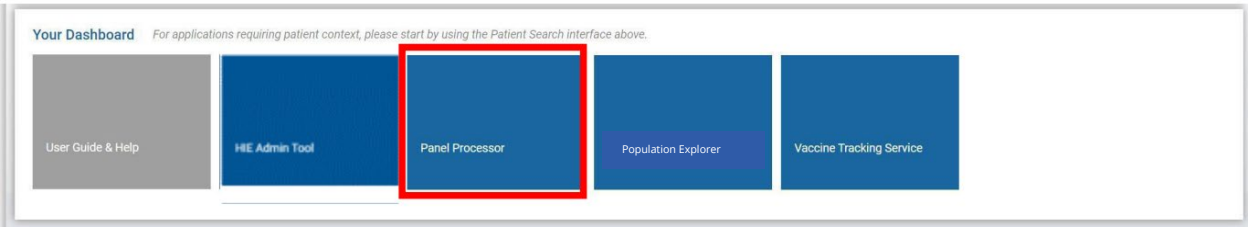


1. Certain
2. Probable
3. Possible



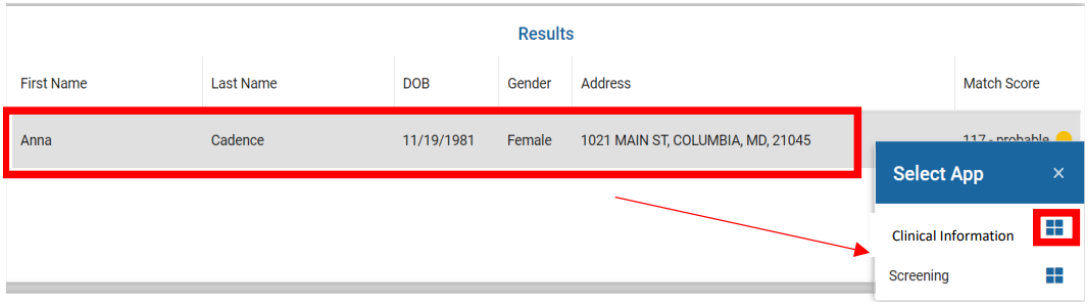
Launching Application

Within the Portal, there are applications which require a patient search and other application 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.



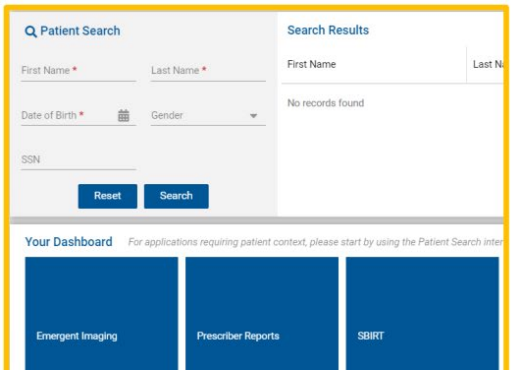
Applications requiring patient context will not appear in Your Dashboard until a patient search is conducted. Once a Patient Search is completed, users can launch their selected patient's data within an application by either:

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.

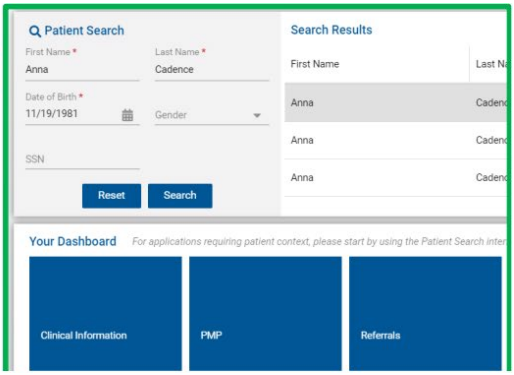


2. Once a patient search is completed and a patient record as been selected, applications that require a patient search will now appear within Your Dashboard. Users can launch these by clicking on the desired application's blue box or tile.

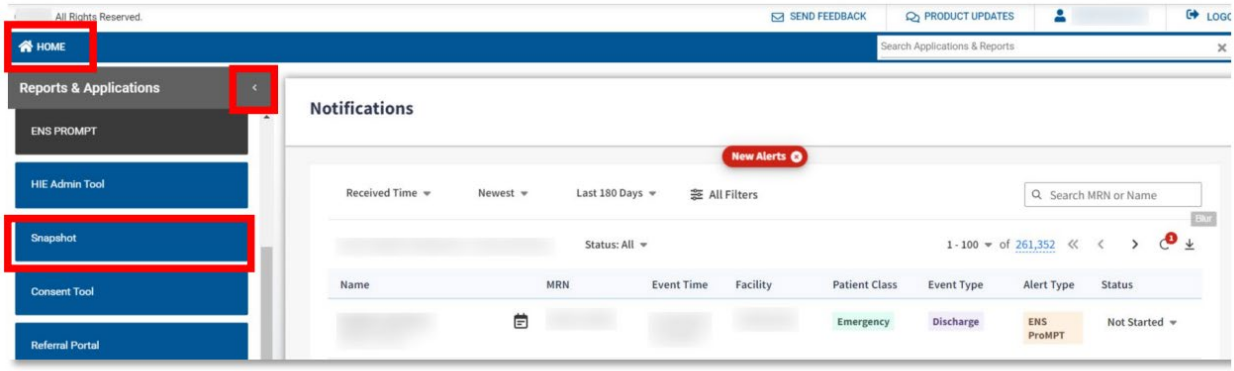
Before a Patient Search

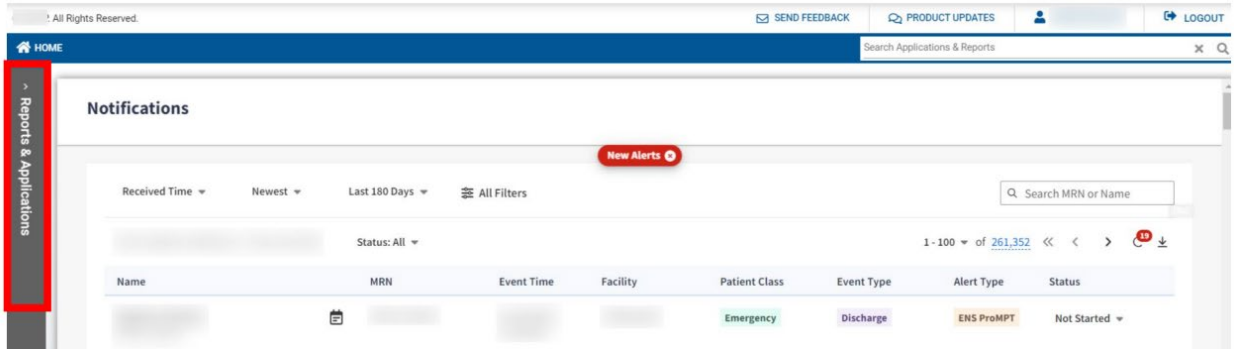


After a Patient Search:



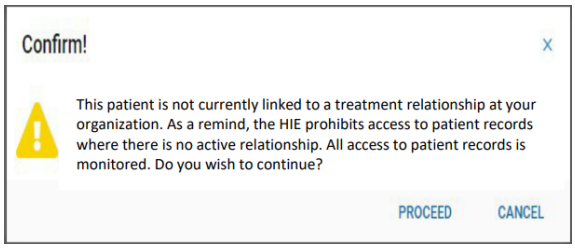
All applications will display within the eye frame of the Portal as shown below. Users can navigate to another application by clicking the application title in the side tool bar. User can collapse the application side menu by clicking on the arrow next to Reports & Applications. The Home button at the top will navigate the page back to the Portal home screen.





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.



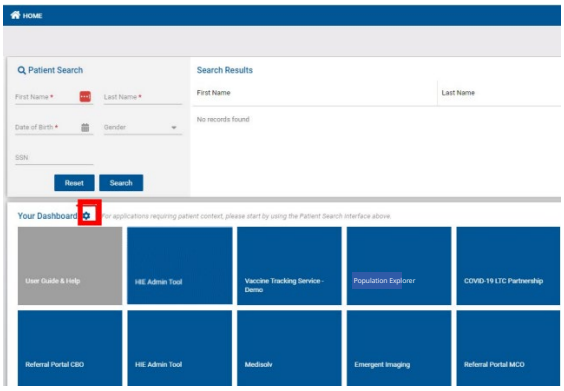
The user can choose to select Cancel, which will navigate the page back to the home screen. If the user selects Proceed, they will be asked to enter a reason for attesting to the relationship. Also, please be aware that all these requests are recorded and audited.

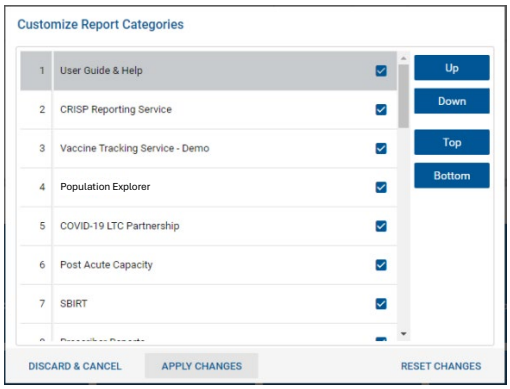
If the patient for whom you are attempting to launch an application has opted out of CRISP, the following message:

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 a random 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 CRISP 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 CRISP. Please reach out to our support staff for questions or clarification.

Technical User Support Contact Information

Support Phone	Email Address	Portal URL
877.952.7477	support@crisphealth.org	https://portal.crisphealth.org

Application Table

The following pages contain two tables listing all CRISP services available for use by users approved by an HIE Admin or by CRISP Support. HIE Admins may or may not have the ability to grant users access depending on your organization type, job role, or participation agreement. Each table below provides information on the service name of the product or application, and a brief description of the service. The first table lists the services an HIE

Admin can credential users to access via the HIE Admin Tool. The second table displays services an HIE Admin may request CRISP Support to provide to a user.

Service	Service Description
Clinical Information	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.
CSS Event Notification Delivery (CEND)	Enables users to receive real-time alerts for patient healthcare events (hospital admissions, discharges, etc.). Event Notifications are primarily delivered via the Population Explorer application, but can also be delivered via HL7, Managed File Transfer SFTP files or via EHR Inbasket.
Consent Tool	Enables users to register patient consent for Substance Use Disorder (SUD) and Mental Health (MH) data on behalf of their patients.
Emergency Department Advisory System (EDAS)	Enables access to show hospital diversion status to support EMS workflows.
MOM Care Plan	Enables Case Managers to create care plans for mothers who are enrolled into the Maternal Opioid Misuse Program.
Population Explorer	Offers a user-friendly interface for clinicians and care teams to review patient encounters from CEND, providing access to the latest encounters and six-month encounter history.
Referrals	Allows users to search Community Based Organizations (CBOs) to find community programs, create a patient referral to a CBO, and manage referrals sent to them all in one application
SBIRT Reporting	MDPCP reporting tool for substance use Screening, Brief Intervention, and Referral to Treatment (SBIRT)
SDOH Screening	Allows users to create assessments for a patient, view previously completed assessments, and view conditions assessed in screenings from other organizations
Snapshot	Enables users to view widgets such as encounter history, medications, diagnoses, procedures and claims data, that provide critical information on their patient. Widgets display an aggregation of both clinical and non-clinical data for the selected patient, pulling information from internal and external sources to provide an at-a-glance view of the patient's clinical history.
SNF Transfer to ED Form	Form approved by all hospitals in MD as an acceptable transfer form.

CRISP

Contact Technical User Support for services listed below:

Service	Service Description
CRISP Reporting Services (CRS)	CRS is currently a stand-alone portal with hundreds of valuable reports and dashboards that support organizations with quality improvement, strategic planning, financial modeling, and other activities. Some organizations have begun transitioning to CRS access via the CRISP Portal. This is an ongoing migration process.
CRISP Reporting Services – Role Manager	Access to the CRISP Reporting Services (CRS) application where these reports are housed is provisioned using Role Manager. Organizations have a CRS Point of Contact who provisions access to summary and/or patient level reports within CRS.
Emergent Imaging	Enables faster, more efficient diagnosis and treatment of strokes. Only members of stroke team at Comprehensive or Thrombectomy Capable Stroke Centers are eligible for access to Emergent, as no patient search is required, and 72-hours' worth of stroke images are made available.
HIE Admin Tool	Allows HIE Administrators to manage user access to the HIE Portal. User account creation or suspension, 90-day audit/user verification, and access to specific HIE Services are handled via the tool.
PDMP Maryland	Access to the Maryland Prescription Drug Monitoring Program data, which monitors controlled substances dispensed by Maryland prescribers.
Prescriber Reports	Access to Prescriber Reports, which include Personal Controlled Substance Prescribing History, Electronic Unsolicited Reporting Notifications and more. Individual DEA required.
Panel Processor	Enables users to upload patient panels to the HIE for CEND, COVID reporting, etc.
Transfer to PACS (TTP)	Allows users to download images into their image storage system, also known as PACs. User access is not automatic and must be approved by a PACS administrator before being granted. Upon request, Technical User Support will reach out to the Image Exchange Project Manager, who will reach out to the PACS Administrator to confirm.