Authorized User Attestation

HealtheConnections Authorized Users are responsible for reading, understanding, and following all requirements listed below. Failure to comply with these requirements will result in consequential actions. By reading these requirements, the Authorized User attests to their understanding.

Authorized User Requirements

HealtheConnections Authorized Users are required to:

- Understand and agree to follow all state and federal privacy and security requirements (including requirements for patient consent) and their organization's guidelines regarding the re-disclosure and use of protected health information (PHI) available through the HealtheConnections Health Information Exchange (HIE).
- Understand that PHI available through the HealtheConnections HIE is limited to that which has been successfully transmitted electronically by connected data sources only.
- Read, understand, and agree to follow HealtheConnections' Privacy and Security Policy and Procedure Handbook. This is located on the HealtheConnections Resource Center under Policy Information.

Users are responsible for independent examination, diagnosis and treatment of a patient. HealtheConnections is not responsible for the completeness or accuracy of information.

HealtheConnections HIE Access and Patient Consent

Consent

Patient consent is normally required to access health information through the HIE (limited exceptions exist, such as disease monitoring by a health department). While patient consent is not required for information to be sent to the HIE, a patient must provide affirmative written consent before their HIE records can be accessed by authorized users. Some instances such as public health reporting and one-to-one exchanges (e.g., Results) do not require patient consent.

- Patient consent is organization-specific; it only applies to the organization that obtained the signed consent form.
- Patients only need to provide consent once but can change their mind at any time by completing a new consent form.
- Providers cannot deny care based on a patient's consent value.
- Consent must be "written" not verbal (dated and signed by the patient on paper, or dated e-signature for an electronic document). If your organization provides remote care via telehealth services additional options to collect consent during these telehealth visits may be available; please contact HealtheConnections to ensure compliance with consent requirements for telehealth.
- A patient's decision not to sign a consent document shall not be construed as "denial of consent."

Consent Values

There are three (3) possible consent values, but most organizations will only have two (2):

- **I give consent –** for the Provider Organization or Health Plan to access ALL of my electronic health information through HealtheConnections to provide health care services (including emergency care)

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

- **I deny consent except in a medical emergency* –** for the Provider Organization to access my electronic health information through HealtheConnections
- **I deny consent –** for the Provider Organization or Health Plan to access my electronic health information through HealtheConnections for any purposes, even in a medical emergency.

**Limited to Designated Organizations that have Break the Glass permissions (see below).*

Consent Actions
There are two (2) consent actions:

- **Break the Glass –** allows designated organizations and specific users (based on role) access to a patient's record in the event of a medical emergency. Once the emergency situation is resolved, the patient's record should only be accessed if they have given their written consent.
    - **Designated organizations** include, but are not limited to hospitals, emergency departments, emergency medical services (EMS).
    - **Authorized users**: Access to this functionality is only allowed for users at a designated organization whose roles require this privilege (e.g., ED personnel, EMTs). Users must complete an AU modification form to request this access, and it must be approved by the organization's RHIO Administrator.
    - **Medical emergency** is defined as when the patient is in need of immediate medical attention and that delaying treatment would increase the risk to the patient's life or health.
    - **Required documentation** of the nature of the emergency (i.e., stroke, myocardial infarction, etc.) and the name of the authorizing provider (e.g., MD, DO) is needed before access can be granted.
    - **Note**: if the patient previously selected "I deny consent," Break the Glass will not be available for that patient.
- **Minor-Consented Services Override –** organizations that provide minor-consented services (MCS) can discuss information and provide treatment to minor patients without parent/guardian permission using the minor-consented services override (MCSO).
    - The parent or guardian is never provided information about the service or the override unless authorized by the minor patient.
    - The override is only effective during the duration of the visit and access to the minor's record expires upon logout within the HIE Portal.
    - The minor cannot override an affirmative consent from a parent or guardian.

Privacy & Security Requirements

Information flowing in and out of HealtheConnections contains Protected Health Information or PHI. Authorized Users must follow SHIN-NY and HIPAA rules when using HealtheConnections, including but not limited to:

- Only access the minimum necessary information
- Follow all re-disclosure requirements (see below)
- Never share login credentials
- Only access individuals with whom you have a treating relationship

As an authorized user of the HIE, you are responsible for understanding and following the applicable laws regarding redisclosure as indicated in the notice on the HealtheConnections Portal log in screen:

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

Redisclosure Notice: The information accessed through HealtheConnections is confidential and may contain sensitive patient information. By logging in and accessing patient records in the health information exchange, you may be viewing patient records that contain Substance Use Disorder protected under SAMHSA 42 CFR, HIV/AIDS protected under Article 27-F of NY Public Health Law or patient records from facilities licensed or operated by the NYS Office of Mental Health for the NYS Office for People With Developmental Disabilities. A general authorization for the release of these data is NOT sufficient and may only be re-disclosed as permitted by state or federal law.

Audits and Compliance

HealtheConnections is a secure system used for exchanging health information. All access to HealtheConnections is recorded and subject to audit. Unauthorized access is prohibited. To ensure compliance is maintained, HealtheConnections works with your organization's RHIO Administrators and Audit Contacts to conduct routine audits.

Failure to comply with privacy and security policies can result in sanctions. Some examples of non-compliance include: using Break the Glass when it is not an emergency, failure to collect written patient consent, looking up yourself/friend/family, and sharing your credentials. Sanctions include, but are not limited to:

- Requiring an Authorized User to undergo additional training
- Temporarily restricting an Authorized User's access
- Terminating the access of an Authorized User
- Suspending or terminating a Participant's participation
- The assessment of fines or other monetary penalties

Login Information

HealtheConnections is a secure system used for exchanging health information. Sharing of usernames and passwords is prohibited.

Security Question

Upon account activation, Authorized Users must complete the required security question to help keep their account secure and make account recovery easier. Users need to:

- Sign in to the HealtheConnections HIE Portal
- Follow the prompts to set up your security question
- Verify your changes and select Continue

Multi-Factor Authentication (MFA)

MFA is an added layer of security designed to ensure that only authorized users can access HealtheConnections resources. MFA requires two forms of verification to help protect your account from unauthorized access.

Additional information can be found in the MFA Methods & Setup guide.

Password Reset

Users will be prompted to change their password periodically. Passwords must meet security requirements and cannot be reused. During this process, if the password is entered inaccurately too many times the user will be locked out and access will need to be reset.

443 North Franklin St., Suite 001
Syracuse, NY 13204
healtheconnections.org

After account setup, users can reset their password and unlock their account, as needed, using the self-service features on the HIE Portal sign-in page. Located below the Sign-In button, users can click the appropriate link and follow the prompts.

If you continue to experience difficulties, please contact us.

Resources & Support

Resource Center

Access guides, documents, and other helpful materials on the Resource Center.

HIE Training Options

- Attend a live session
- Watch an on-demand video
- Read through the HIE User Guide

HIE Portal Help Center

Within the HIE Portal, users have quick access to system notifications, training and resources, and support information in the Help Center.

News & Updates

HealtheConnections will send information and updates directly to you. Subscribe here.

HealtheConnections Support

Phone: (315) 671-2241 ext. 5
Email: support@healtheconnections.org
Website: healtheconnections.org

443 North Franklin St., Suite 001
Syracuse, NY 13204