Authorized User Policy and Procedure Training
Agenda

- Welcome to HealtheConnections
- HIE By the Numbers
- Our Services
- Access
  - Access at multiple organizations
  - Emergency Access
  - Authorized User Form
- HIPAA & the HIE
- Consent
  - Consent Process
  - Sample Consent
  - Consent Values
  - Community-Wide Deny
  - Minor-Consented Services
- Audits
- Demo of the system and/or HIE User Manual review*

*HIE User Manual review only required for self-training, along with Policy & Procedure
HIE By the Numbers

- 6 million patients able to receive better care
- 1,400 organizations connected to the HIE
- 100% of hospitals connected to the HIE
- 3,400 locations connected to the HIE
- 26-county service area

3,400 locations connected to the HIE

26-county service area

1,400 organizations connected to the HIE

100% of hospitals connected to the HIE

6 million patients able to receive better care
Our HIE Services

- **Image Exchange**: Diagnostic-quality images directly delivered to you
- **Query-Based Exchange**: Access information through state and national databases
- **Patient Lookup**: Real-time patient records at the touch of a button
- **Direct Mail**: HIPAA-compliant secure mail & national provider directory
- **Results Access & Delivery**: Labs, rads, and reports easily accessed or delivered directly
- **myAlerts**: Clinical alerts for hospital admits, discharges, and more with extensive filtering capabilities
• Access to patient records is given to Authorized Users at the organization level

• Users will need to complete an Authorized User form and receive annual refresher training

• The RHIO Administrator for each public health organization is responsible for contacting HealtheConnections regarding the activation and deactivation of authorized users
• Users who work at multiple organizations will only need one username and password
• After logging in, the user will have a specific badge for each organization that they work on behalf of
• It is extremely important to choose the correct facility when utilizing “Patient Lookup”
• Patient consent applies only to the organization at which it was given
A limited number of MD’s and DO’s will have unique access to a feature called “Break the Glass”.

“Break the Glass” access may only be used to access a patient record in the case of emergencies that require emergency treatment, in accordance to Public Health Law Section 2504(4).

If a user with this security role uses the “Break the Glass” feature, an audit will automatically be generated.

All “Break the Glass” audits will require a response from the organization’s RHIO Administrator.

LIMITED users will have access to “Break the Glass”.
Authorized User Form

Authorized User Certification and Application

* Indicates required field. Copy of this form must be kept on file for 8 years by the requesting organization.

* Last Name
* First Name
* Middle Initial

* Title
* Credentials. If any (MD, DO, etc.)

* Participating Organization
* Department (if applicable)

* Street Address of Participating Organization
* City
* State
* Zip

* Unique Email Address (work email preferred)
* Phone Number

* Preferred User Name:
(existing or previous HIE user account information:
[ ] Currently Employed OR [ ] Previous Employed Elsewhere with Access
Organization Name:
Username:

REQUIRED for Prescribing Clinicians:

APL

* Training Method
[ ] RHIO-led training
[ ] Facility staff-led training
[ ] Self-trained

* Training Completion Date:

* Patient Lookup Access Type
[ ] Clinical records
[ ] OR
[ ] Patient Demographics Only
[ ] OR
[ ] Public Health (only available for PH organizations)

Break the Glass Access is not granted to all users by default.
If you require Break the Glass Access, please complete supplemental BTO request form (subject to review).

* Additional Options (check with your RHIO Administrator for available options)
[ ] Secure mail
[ ] Transfer to PACS (TPP)
[ ] Alerts (Complete Alert Form)
[ ] Community Referrals **
[ ] SSO (provide杜兰ian Username)
[ ] myResults (including delegation - Complete myResults Form)
[ ] Perinatal Referrals
[ ] RHIO Administrator
[ ] Audit Report Recipient

** Secure Mail Address for Community Referrals (leave blank if requesting new HealthConnections Secure Mail account):

By signing this document, I confirm that I have completed HIE training, read & understood the HIE access policies & I am requesting an HIE account.

Signature:
Date:

Photo ID Type (e.g., Driver’s License, Employee Badge):

ID Number:

By signing this document, I, the RHIO Administrator, HealthConnections trainer or other authorized individual certify that the identity of this user has been proven:

Authorizing Signature:
Date:

Authorizing Signature’s Email Address:
Title:

PLEASE SUBMIT TO SUPPORT@HEALTHCONNECTIONS.ORG OR FAX TO 1-315-407-0053.

Authorized User Certification and Application_03_01_2019 1 | Page
Protected Health Information (PHI) is any individually identifiable health information, which may include sensitive health conditions including, but not limited to:

- Substance Use Disorder
- Birth control and abortion (family planning)
- Genetic (inherited) diseases or tests
- Any mention of HIV/AIDS
- Mental health conditions
- Sexually transmitted diseases

**Redisclosure Notice:** Any patient records that are accessed through HealtheConnections’ health information exchange are subject to all applicable federal and state laws for redisclosure, including but not limited to Minor Consented Services, Substance Use Disorder, HIV/AIDS, Mental Health, and Developmental Disabilities. If such information is present in the HIE, law prohibits you from making any further disclosure of this information without the written consent of the person to whom it pertains. A general authorization for the release of medical or other information is NOT sufficient for this purpose. As an authorized user of the HIE, you are responsible for understanding and following the applicable laws.
HIPAA privacy and security rules must be followed for using the HIE, including, but not limited to, rules such as:

- Minimum Necessary Access
- Redisclosure requirements (State and Federal)
- Do not share your login credentials with anyone
- Do not look up yourself, family members, or friends
- **Looking up your own record is a VIOLATION and will create an AUDIT**

PHI should be securely shared using one of the following methods:

- Direct Mail
- Fax
- Email – **only** if the PHI file is encrypted and/or password protected

For more information about HIPAA policy, visit: [http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)
NYS law requires that Participating Organizations obtain a patient’s consent before viewing their PHI for non-emergency treatment

- HIE records may only be viewed for patients who provide an affirmative consent

- A patient’s consent applies only to the Participating Organization that collected the consent form, not to all Participating Organizations
  - Patients only need to provide consent for a Participating Organization **one time**
  - A patient may change their consent value at any time by filling out a new consent form at each Participating Organization

- For non-public health access, NYS law requires each participating organization to obtain a patient’s consent before viewing their PHI for non-emergency treatment

- A patient’s consent applies only to the participating organization that collected the consent form, not to all participating organizations

- Any authorized user at the participating organization may access a consenting patient’s health record, with the appropriate security role

- Providers cannot refuse treatment to patients based on willingness to provide consent
## Sample Consent

### Authorization for Access to Patient Information through a Health Information Exchange Organization

<table>
<thead>
<tr>
<th>Patient Name</th>
<th>Date of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I request that health information regarding my care and treatment be accessed as set forth on this form. I can choose healthie.com to allow SAMPLE to obtain access to my medical records through the health information exchange organization called HealthieConnections. If I give consent, my medical records from different places where I get health care can be accessed using a statewide computer network. HealthieConnections is a not-for-profit organization that shares information about people's health electronically and meets the privacy and security standards of HIPAA and New York State Law. To learn more visit HealthieConnections website at [http://healthieconnections.org](http://healthieconnections.org).

My information may be accessed in the event of an emergency, unless I complete this form and check box #3, which states that I deny consent even in a medical emergency.

The choice I make in this form will NOT affect my ability to get medical care. The choice I make in this form does NOT allow health insurers to have access to my information for the purpose of deciding whether to provide me with health insurance coverage or pay my medical bills.

### My Consent Choice: ONE box is checked to the left of my choice

- **1. I GIVE CONSENT for SAMPLE to access ALL of my electronic health information through HealthieConnections to provide health care services (including emergency care).**

- **2. I DENY CONSENT EXCEPT IN A MEDICAL EMERGENCY for SAMPLE to access my electronic health information through HealthieConnections.**

- **3. I DENY CONSENT for SAMPLE to access my electronic health information through HealthieConnections for any purpose, even in a medical emergency.**

If I want to deny consent for all Provider Organizations and Health Plans participating in HealthieConnections to access my electronic health information through HealthieConnections, I may do so by visiting HealthieConnections website at [http://healthieconnections.org](http://healthieconnections.org) or calling HealthieConnections at 315.671.2261 x5.

My questions about this form have been answered and I have been provided a copy of this form.

<table>
<thead>
<tr>
<th>Signature of Patient or Patient’s Legal Representative</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Print Name of Legal Representative (if applicable)</th>
<th>Relationship of Legal Representative to Patient (if applicable)</th>
</tr>
</thead>
</table>
Consent Values

- **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)

- **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 purpose, even in a medical emergency
Community-wide Deny Consent

- If patient requests “Community-wide Deny” consent, the following options are available:
  - The patient completes a Community-wide Deny consent form and your organization submits to HealtheConnections Support to enter the consent
  - The patient can visit the HealtheConnections office, with photo identification to complete the form and enter the consent
  - The patient can take the form and have it notarized and send it to HealtheConnections Support, who will enter the consent
Who can sign consent?

- **Patients under 18 years**: Parents, Legal Guardians, or State Officials can sign the consent form on behalf of the patient.
- **Patients aged 18+ years**: May provide consent for themselves.
- **Health proxy/representative**: If an agent is appointed by a patient in a health proxy document or due to incapacity to legally make healthcare decisions on behalf of the patient, that agent may provide consent for the patient.
Patients under 18 years old can override parental/guardian consent for a minor consented service

- An override can only take place if the parent/guardian has not yet consented or has selected “Deny” or “Deny, Except in an Emergency”
  - A minor cannot override a “YES” consent provided by a parent or legal guardian
  - FAQs are available for minor consent override

- To activate the override, a minor must sign an override consent form to give the participating organization permission to access his/her health records only when the minor is physically present

- The override will only remain in effect for the duration of the visit and will expire when the authorized user logs out of the patient’s record when the encounter is complete
Consent Exceptions

Consent is *NOT* required for:

- Data sources sending patient medical records to the HIE
- One-to-One Exchanges (Results Delivery)
- Emergency situations, if patient has not yet consented, or has not selected “Deny to the Participating Organization” or “Community-wide Deny” consent
- De-identified Data
- Public Health access
Patient consent can be captured in two ways, depending upon your facility’s capabilities:

- Most facilities log into HealtheConnections Patient Lookup and enter the patient’s consent directly into the HIE
- Hospitals and some practices capture patient consent in their EHRs, which is then sent over electronically to the HIE
Maintaining Consent Forms

- Patient consent forms must be kept with a patient’s record for six (6) years.
- Signed paper consent forms can be stored in patient charts OR electronic (scanned) copies of the consent forms can be kept on file.
- Consents are subject to periodic auditing:
  - A copy of the patient’s signed consent form must be made available in the event of an audit.
Audits

- Access to patient records are audited:
  - Break the Glass events are audited daily
  - Public Health non-consented access is audited weekly
  - Each Participating Organization is required to attest to an annual audit of patient consents, user accesses of patient information, and user logins
  - Audits may be triggered by same name logic
  - Patients can request audits of access to their own records
    - This can be done via a participating organization or by contacting HealtheConnections
Accessing HealtheConnections

Please visit [www.HealtheConnections.org](http://www.HealtheConnections.org) to learn more about us.
Click on “myConnections Login” to access our portal.
Important Information

HealtheConnections Support:
• Email: support@healtheconnections.org
• Direct Email: support@hiemail.healtheconnections.org
• Phone: 315-671-2241 ext. 5

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Business Hours</th>
<th>Off Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Immediate</td>
<td>Immediate</td>
</tr>
<tr>
<td>Voice Mail</td>
<td>2 hrs</td>
<td>4 hrs</td>
</tr>
<tr>
<td>e-mail</td>
<td>4 hrs</td>
<td>Next Business Day</td>
</tr>
<tr>
<td>Fax</td>
<td>4 hrs</td>
<td>Next Business Day</td>
</tr>
</tbody>
</table>

Training Materials:
• HIE User Manual accompanies the Authorized User Training
• Additional materials and forms are available on our website, under the Health Information Exchange Training & Documents section

myConnections:
• Use “Forgot Password” on the myConnections login page for password resets
Thank You