HealtheConnections™

RHIO Administrator Training

History of HealtheConnections

- Formed in 2010 as the Regional Health Information Organization (RHIO) for HealtheConnections
- Manages and oversees the Health Information Exchange (HIE)
- HIE is the single access point for healthcare providers to view a patient's medical records
- 700+ participants in 11-county region
- Over 200 organizations contribute data directly to the HIE

Our Services

Patient Lookup

Real-time consolidated view of a patient's comprehensive health records

Direct Mail

Secure email system to communicate patient clinical information between healthcare professionals

Image Exchange

Access to and viewing of diagnostic-quality radiology image studies. Compare multiple studies at once and transfer images into radiology systems

myAlerts

Patient activity notifications sent to providers for emergency department encounters, in-patient hospital admissions and discharges

Query-Based Exchange

Access to statewide patient data from other RHIOs and New York State sources, as well as federal government data sources (VA and DoD)

Results Access & Delivery

Automated delivery of results, reports, and images through the HIE either to an EHR or through the myResults tab in the myConnections portal

RHIO Administrator Appointment

- Participating Organizations must appoint at least one person as a RHIO Administrator (RA)
- RA will be the point of contact for HealtheConnections Support Staff, Provider Engagement Specialists (PES), and staff within the Participating Organization
- RA will be the only authorized staff to contact HealtheConnections Support to perform specific functions
- An assigned PES team member will meet with the RA in person to ensure the role is understood and implemented appropriately
- RA is expected to communicate all updates or other communication and additional requests from HealtheConnections to Authorized Users (outside of Audit Report Requests)
- RA will delegate requests internally within the Participating Organization as needed

Protected Health Information (PHI)

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

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

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

Patient Education

- HealtheConnections and its Participating Organizations are required to educate patients on the informed consent process and the terms and conditions by which protected health information (PHI) is shared
- HealtheConnections offers an informed consent script for staff to utilize when asking patients to sign the consent form

Consent

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
- Participating Organizations must inform patients that ANY and ALL health information included in their health record will be available through the HIE
  - Direct patient to HealtheConnections.org/map
- 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

Consent Values

Basic 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

If a patient requests “Community-wide Deny” consent, the following options are also 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
- The patient can take the form and have it notarized and send it to HealtheConnections Support
- Ensure the patient understands the impact of Community-wide Deny

Who can sign consent?

- **Patients under 18 years:** Parents, Legal Guardians, or State Officials can sign the consent form on behalf of 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

Consent Exceptions

Consent is not required for:

- Data Sources sending patient medical records to the HIE, except for Substance Use Disorder (CFR 42)
- One-to-One Exchanges (Direct Mail)
- 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

Capturing Consent

Patient consent can be captured in two ways, depending upon your facility's capabilities:

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

Minor Consented Services Access Override

Patients under 18 years old can override parental/guardian consent for a minor consented service **only**

- 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 “Give” consent provided by the parent/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

Emergency Access

- **“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)
- The Practitioner determines, in his or her reasonable judgment, that information that may be held by or accessible through the HIE may be material to emergency treatment

Managing Authorized User Accounts

RHIO Administrators are responsible for:

- Authentication/identity proofing of Authorized users within the organization
- Ensuring all training is completed prior to approving an Authorized User account – **SEE P. 29 FOR TRAINING REFERENCE**
- Requesting scheduled on-site trainings
- Ensuring a process is in place to retain Authorized User forms for six (6) years
- Notifying HealtheConnections Support to terminate access for Authorized Users who no longer require access to the HIE
- Managing annual refresher trainings

Authorized User Access Types

Clinical

- Access to all patient records in the HIE
  - Patient demographics, lab results, radiology reports and images, medications, allergies, etc.
- Best for: physicians, nurse practitioners, physician assistants, nurses, other clinical and medical support staff

Patient Demographic Only

- Access to patient demographics **only**
  - Name, address, and insurance information
- Best for: registration or admission staff who are responsible for entering consent for a facility

Public Health

- Additional privilege for users within the health departments who require a non-consenting role

Patient Management

- Manage and retain patient consent forms for six (6) years
- Contact HealtheConnections Support for patient merges, unmerges, or inaccurate data
- 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 HealtheConnections office, with photo identification to complete the form
  - The patient can take the form and have it notarized and send to HealtheConnections Support

Practice/Organization Management

- Liaison to the organization for HealtheConnections notifications, updated materials, roll-out of new features/functionalities, and all types of information requests
- Notify HealtheConnections of any changes within the organization:
  - Practice closure
  - User account activation/deactivation
  - Acquisition by/merger with another organization
  - EHR vendor change (e.g. change of system, product name, etc.)
  - New services being offered by the practice
  - Maintain updated physician list (MDs and DOs)

Audit Report Management

- Receive, review, and attest to audit reports*
  - Submit patient consent forms as part of a random sampling audit
  - Validation of a random sample of Authorized Users to ensure identity proofing

*This responsibility may be designated to another individual (e.g. compliance officer or policy officer) rather than RA and is referred to as the Audit Report Recipient (ARR)

Audit Report Management

- Receive, review, and attest to daily Break the Glass reports*
- Annual Refresher Training attestation
- Report breaches and assist HealtheConnections with resolutions
  - Participating Organization may request an audit in the event of a suspected breach

*This responsibility may be designated to another individual (e.g. compliance officer or policy officer) rather than RA and is referred to as the Audit Report Recipient (ARR)

Direct Mail Management

- Completion of DigiCert form
- Provide list of Authorized Users for Direct Mail account set-up
  - All users can be set up with Direct Mail
  - Only providers can delegate access to staff (staff cannot delegate, and providers cannot delegate to another provider)
- Facilitate workflow development with other organizations

myAlerts Management

- Determine which alert types best fit the organizational workflow
- Provide a list of Authorized Users with usernames and Direct Mail addresses for myAlerts set-up
- Maintain patient subscription file

Results Access & Delivery Management

- Assist in project initiation with EHR vendor
- Provide list of NPIs to EHR vendor and HealtheConnections for Results Deliver set-up
- For myResults users: complete delegation access form
- Discuss data source options

Breach Management

HealtheConnections and its Participating Organizations must notify each other of any actual or suspected breaches

- HealtheConnections and the Participating Organization will investigate all incidents
- HealtheConnections will:
  - Notify Participating Organization if PHI was subject of a breach
  - Notify, or require Participant to notify, the patient(s) whose PHI was breached
  - Notify any applicable regulatory agencies, as appropriate
  - Determine disciplinary and/or other sanctions, as appropriate

Policy Compliance

Participating Organizations shall implement sanctions and hold workforce accountable for complying with the Policies & Procedures

- Violation of policy must be reported to the entity's privacy officer and HealtheConnections
- Disciplinary measures may include written warnings, re-training requirements, and termination of participating in the HIE

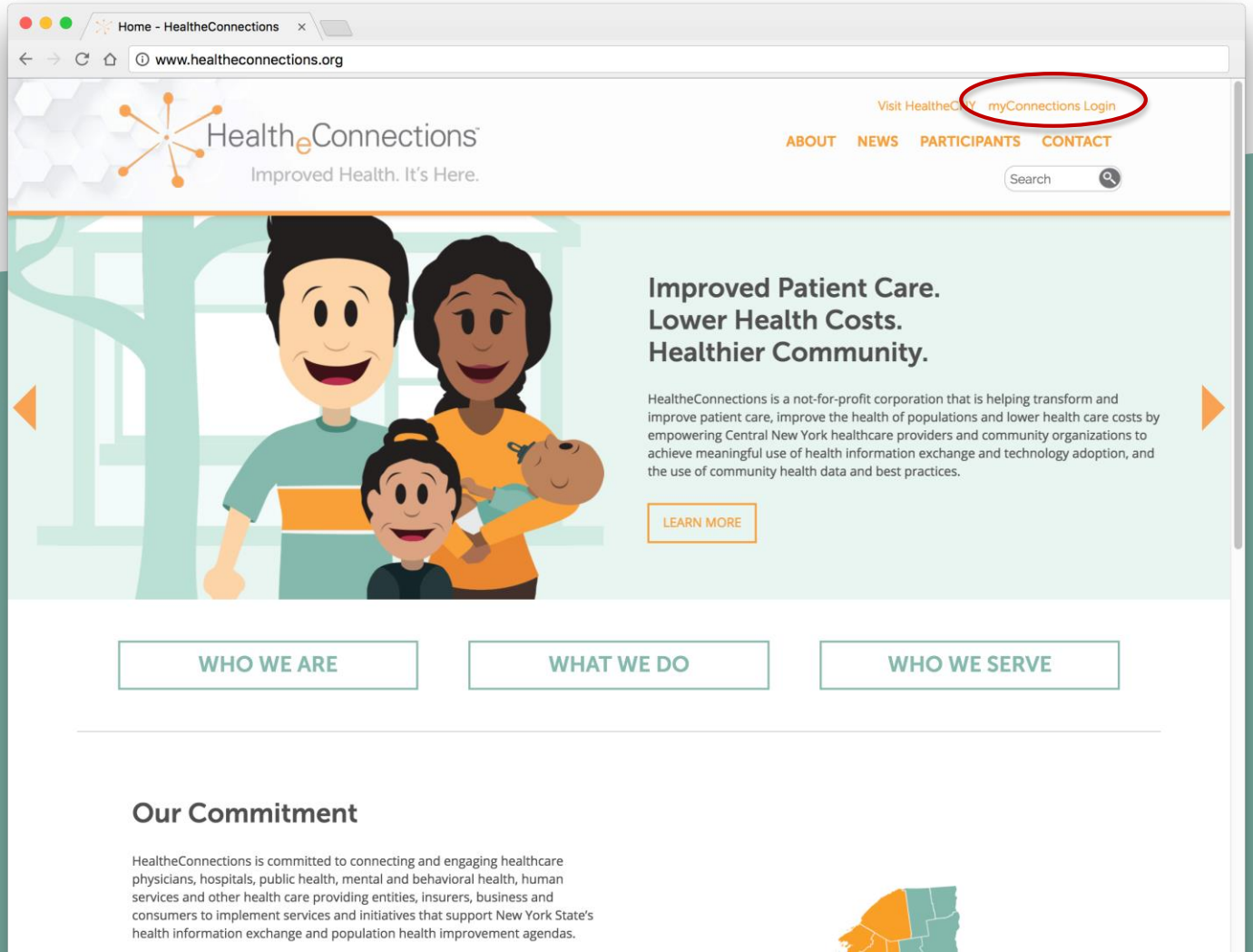
Access at Multiple Facilities

- Users will only need one* username and password; however, when logging in, the user must select the facility for which patient records are being accessed
- Patient consent applies only to the facility at which it was given

* Public health users may require two (2) sets of login credentials if they use the HIE as both a Clinical Authorized User (consent required) and as a Public Health Authorized User (consent not required)

Accessing myConnections

From the HealtheConnections homepage, click on “myConnections Login” link and enter username and password to log in



Important Information

HealtheConnections Support:

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

Training Materials:

- HIE User Manual accompanies the Authorized User Training
- Additional materials and forms are available at: http://www.healtheconnections.org/what-we-do/hie-services/training-materials/

myConnections:

- Use “Forgot Password” on the myConnections login page for quick and easy password resets

For more information, visit:
www.healtheconnections.org