Healthix

EXCHANGING INFORMATION
TO TRANSFORM PATIENT CARE

Healthix Required Policy Training Telehealth

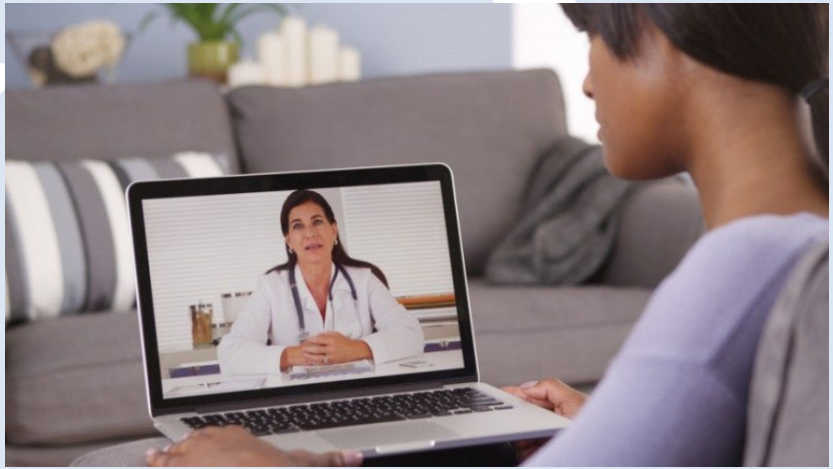
2025

Healthix

Telehealth and Verbal Consent to Access Healthix Data

The State Health Information Network of New York (SHIN-NY) and Healthix adopted policies that allow Providers who engage in telehealth services to obtain a “verbal” consent from a patient for access to data stored in SHIN-NY database via Healthix.

HIPAA imposes privacy requirements for telehealth, ensuring the protection of patient data during remote encounter with a provider. One such measure, is role-based access control (RBAC).



Healthix designed a specific user role that will allow one time access based on verbal consent obtained during telehealth encounter.

Healthix

Conditions of Access via Verbal Consent

Criteria for use:

- The User must be authorized by a Participant to access patient information via Healthix, AND
- The User must be provisioned as a telehealth provider (telehealth role) by the dedicated AUM (Authorized User Manager), AND
- The User must be engaging patients via telehealth encounter for purposes of treatment or care management (e.g., primary care, behavioral health, case management visit, etc.) AND
- The patient should understand that consent is being granted to access clinical records stored in Healthix prior to the search for data.

Required Documentation:

- All verbal consents for access to the Healthix/SHIN-NY must be documented by the Participant in patient record (e.g., Telehealth encounter note) prior to accessing the patient's data via Healthix.
- The documentation should explicitly indicate that Patient granted the user access to their Healthix records not that they have consented to a telehealth visit.
- The supporting documentation must include the date the verbal consent was obtained from the patient.

Healthix

Teleheatlh and Verbal Consent to Access Healthix Data

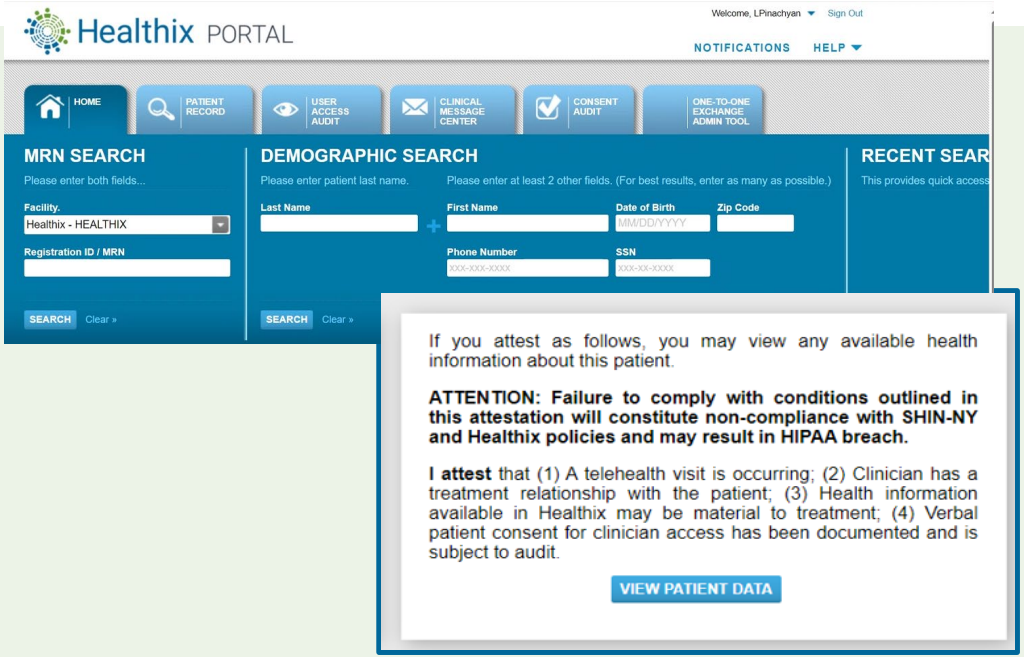
Please note the following limitations:

- **Access based on verbal consent will not allow providers to see data subject to 42 CFR Part (Substance Use Disorders) or data originating from OMH licensed programs/facilities.**
- **If prior to telehealth encounter the patient filed a DENY consent with the organization that the Authorized User is working for the user will not be offered the ability to access the data in Healthix.**
- **Similarly, if a patient filed a DENY ALL request with Healthix that prevents all Participants of Healthix and their authorized users to access that patient data in our database, the user will also not be offered the option to override this consent decision vial verbal consent obtained during telehealth encounter.**

Healthix

What is the Healthix Telehealth Consent Workflow?

1. Log in to Healthix web based portal.
2. Search for patient.
3. Review the attestation in the telehealth prompt window (4 conditions).
4. Proceed with attestation if all 4 conditions are met, **OR do not proceed** with the attestation and **exit** the patient record if all 4 conditions for access are not met.



REMINDER: this telehealth prompt will only appear if the provider has been assigned a telehealth role.

Healthix

Inappropriate Uses of Telehealth Consent Workflow

Below are examples of inappropriate access that will result in sanctions:

- **Not engaging in a telehealth visit with the patient.**
- **Not documenting the verbal consent for access to Healthix in the internal files (local medical record).**
- **Obtaining verbal consent after the telehealth access was executed.**
- **Accessing Healthix data on someone other than your telehealth patients.**
- **Accessing your own data via telehealth.**

If you are unsure why you are seeing the Telehealth pop-up, please reach out to the Healthix Compliance department compliance@healthix.org for clarification prior to selecting “View Patient Data” and accessing PHI.

Healthix

DID YOU KNOW?

The type of sanction that will be applied will be based on progressive corrective action and will take into consideration the type of violation and other key factors such as:

CONSIDERATIONS WHEN APPLYING SANCTIONS

- Non-Intentional/ Minor Violations
- Intentional, Egregious or Substantial Violations

BASES FOR SANCTIONS

- Number of Violations
- Culpability
- Criminal Indicators
- Harm

Healthix

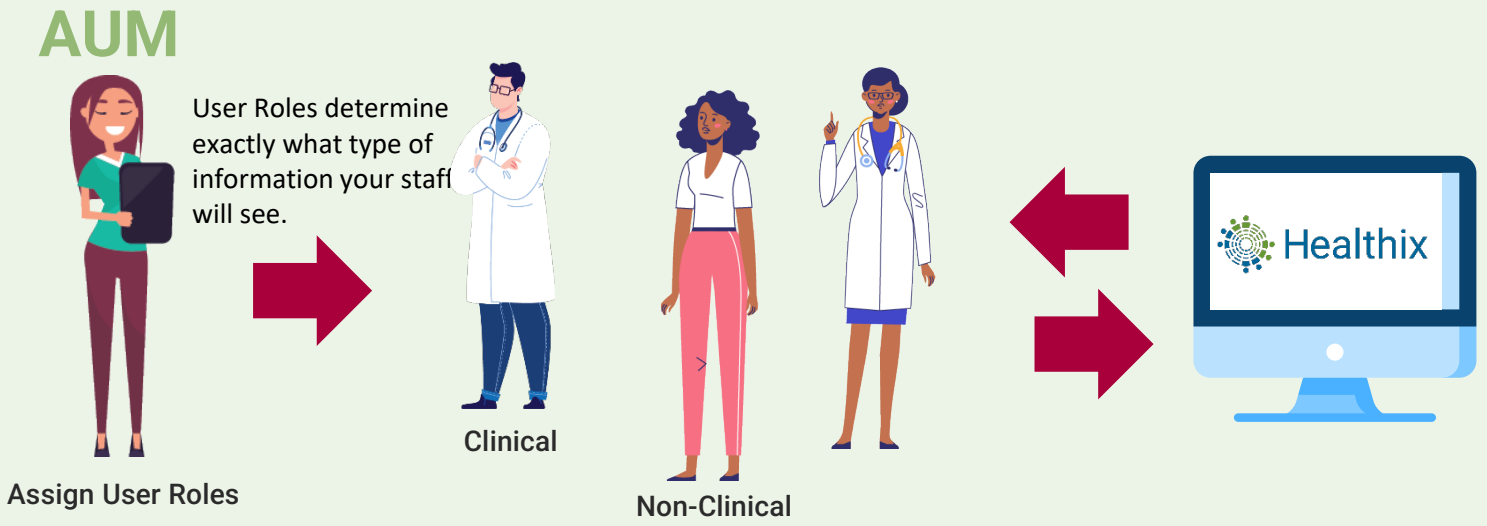
Sanctions for Inappropriate Access – Progressive Corrective Action

Violation	Sanction
Violation of SHIN-NY or Healthix policy not rising to HIPAA violation (e.g., self-search, BTG access, telehealth access).	**1st violation:** temporary suspension of user and re-education. **2nd violation:** temporary suspension, written warning and re-education. **3rd violation:** permanent suspension of user from accessing Healthix and SHIN-NY.

Note: if the investigation of a user's access results in actual Breach of Patient Protected Health Information the user will be permanently deactivated, and the event will be subject to reporting to state and federal agencies.

Healthix

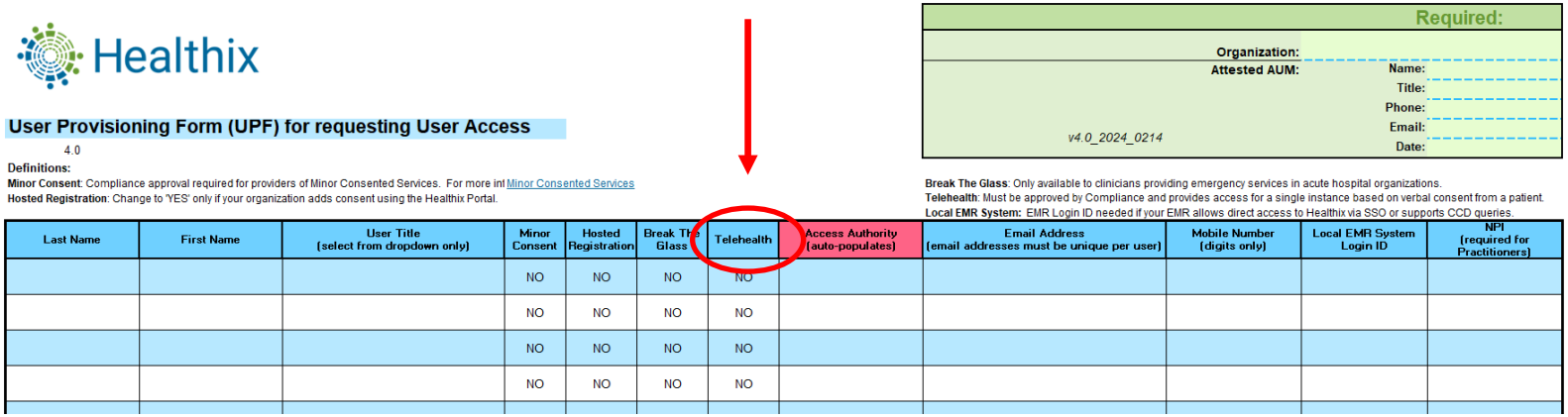
Every Participant of Healthix is required to have an Authorized User Manager (AUM).



Healthix

Requesting Telehealth Access Role

- Authorized User Managers (AUMs) are required to complete telehealth training to understand who should be assigned telehealth role.
- AUMs are responsible for assuring that users perform telehealth visits and thus require telehealth access.
- The provisioning form must be completed and submitted to Healthix to provide users with telehealth access via the portal.
  - Choose “Yes” under Telehealth column header - it will trigger Telehealth training requirement for specific users.
- Questions that AUMs may have should be directed to the Healthix Relationship Manager and/or to compliance@healthix.org.



Healthix

User Provisioning Form (UPF) for requesting User Access

4.0

Definitions:

Minor Consent: Compliance approval required for providers of Minor Consented Services. For more int Minor Consented Services

Hosted Registration: Change to 'YES' only if your organization adds consent using the Healthix Portal.

Required:

Organization:

Attested AUM:

Name:

Title:

Phone:

Email:

Date:

v4.0_2024_0214

Break The Glass: Only available to clinicians providing emergency services in acute hospital organizations.

Telehealth: Must be approved by Compliance and provides access for a single instance based on verbal consent from a patient.

Local EMR System: EMR Login ID needed if your EMR allows direct access to Healthix via SSO or supports CCD queries.

Last Name	First Name	User Title (select from dropdown only)	Minor Consent	Hosted Registration	Break The Glass	Telehealth	Access Authority (auto-populates)	Email Address (email addresses must be unique per user)	Mobile Number (digits only)	Local EMR System Login ID	NPI (required for Practitioners)
			NO	NO	NO	NO					
			NO	NO	NO	NO					
			NO	NO	NO	NO					
			NO	NO	NO	NO					

Healthix

Attestation

Now it’s time to complete the attestation. You are stating that you understand your role and responsibilities. This will trigger a congratulatory email letting you know you can access Healthix data. If you are a new portal user, the email will also contain instructions on how to complete your first successful login.

See you in a year for annual refresher training.

Thank you.

Healthix

Healthix

EXCHANGING INFORMATION
TO TRANSFORM PATIENT CARE

Thank You!
Your training is complete

Any Questions:
compliance@healthix.org

Healthix