

Privacy Impact Assessment (PIA)- Ticketing System

Introduction

This Privacy Impact Assessment covers HealthConnections' ticketing system which is used to track requests or complaints related to 1) "Authorized Users" of HealthConnections' systems and 2) "Patient Requests" including requests for audit log information or a copy of clinical records.

Section 1.0

The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information requested and/or collected as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information may be collected?

1.1.1 For Authorized Users: Individual's Name, Email, Phone, Title, Credentials, NPI, and Username, plus the Name and Address of the Participating Organization with which they are affiliated.

1.1.2 For Patient Requests: Requestor's name; Requestor's relationship to patient (proof of legal authority to make the request on behalf of a Patient), Patient name, Patient date of birth, Patient home address, Patient email address, Recipient name, Recipient address, Recipient email address

1.2 From whom is the information collected?

1.2.1 The individual who makes a request or complaint.

1.3 Why is the information being collected?

1.3.1 For Authorized Users: Information is being collected so that HeC can 1) verify the individual's identity and right of access; 2) respond to the request or complaint.

1.3.2 For Patient Requests: Information is being collected so that HeC can 1) verify the individual's identity; 2) respond to the request or complaint.

1.4 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

1.4.1 Identity proofing for Authorized User accounts and to respond to Patient Requests is required by New York State regulation ([10 NYCRR § 300.3\(b\)\(1\)](#))

Section 2.0

Uses of the System and the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all uses of the information.

2.1.1 Information is being collected so that HeC can 1) verify the individual's identity; 2) verify the individual's right to the information they are requesting; 3) respond to the request or complaint; 4) For Authorized Users: to provide updates and training on Policies and Procedures for accessing HealthConnections' systems; 5) For Authorized Users: to verify the accuracy of their information (for example, to periodically ensure they are still affiliated with a Participating Organization and still eligible to access HealthConnections' systems).

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

2.2.1 N/A. HealthConnections does not mine this data.

2.3 How will the information collected from individuals or derived by the system, including the system itself be checked for accuracy?

2.3.1 For Authorized Users: Authorized Users' information is verified by the main contact at the Participating Organization, known as the "RHIO Administrator" to ensure 1) the identity of the person requesting credentials matches the person for whom credentials are requested (i.e., the RHIO Administrator is responsible for identity proofing); 2) the individual requesting access is affiliated with the Participating Organization; 3) the individual requesting access requires this access to perform their job functions.

2.3.2 For Patient Requests: Patient identity is confirmed whenever Patient Request(s) are filled out (identity proofing is done separately for each request). Identity proofing is completed by one of the following individuals 1) a Notary Public; 2) the patient's provider who is a Participant with HealthConnections; or, 3) HealthConnections staff. When done by a Notary Public or patient's provider, they shall follow their own procedures to adequately identity-proof the individual. When done by HealthConnections, this is done by a comparison of the individual's government-issued photo identification with the individual's likeness and/or demographic information on the form. Once the patient identity is confirmed, HealthConnections' will match demographic information on the Patient Request form to the demographic information in our system to locate the patient record that is the subject of the request.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

3.1.1 The retention period for Authorized User requests and Patient Requests is a minimum of 6 years.

3.1 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

3.1.2 HealtheConnections is not subject to NARA. HealtheConnections is governed by New York State regulation ([10 NYCRR § 300.3\(b\)\(1\) v4.1](#)), which stipulates a retention period of a minimum of 6 years.

Section 4.0

Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing within HealthConnections.

4.1 With which internal organization(s) is the information shared?

4.1.1 The information is received by the Customer Support and Advisory Services and shared with internal personnel who fulfill the patient request, including Operations & Compliance team and the Solutions & Engineering team.

4.2 For each organization, what information is shared and for what purpose?

4.2.1 The individual's demographic information is shared so that HealthConnections' workforce members can respond to the request or complaint.

4.3 How is the information transmitted or disclosed?

4.3.1 Information is maintained in our Support Team's ticketing system and the ticket is assigned to workforce members who are responsible for responding to the request or complaint.

Section 5.0

External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to HealthConnections which includes Federal, state and local government, and the private sector.

- 5.1 With which external organization(s) is the information shared?
 - 5.1.1 For Authorized Users: Information is shared with their affiliated Participating Organization so that the validity of the request can be verified.
 - 5.1.2 For Patient Requests: Information is not shared externally except as specified by the individual on the Patient Request form.
- 5.2 What information is shared and for what purpose?
 - 5.2.1 For Authorized Users: The Authorized User request or modification form is shared so that the validity of the request can be verified.
 - 5.2.2 For Patient Requests: Information is only shared externally to comply with the instructions provided by individual on the Patient Request form.
- 5.3 How is the information transmitted or disclosed?
 - 5.3.1 For Authorized Users: The Authorized User request or modification form is transmitted to the RHIO Administrator via AdobeSign for approval.
 - 5.3.2 For Patient Requests: Information is transmitted or disclosed in the manner indicated by the individual on the Patient Request form.
- 5.4 Is a contract, or agreement in place with any external organization(s) with whom information is shared, and does contract reflect the scope of the information currently shared?
 - 5.4.1 For Authorized Users: A Participation Agreement (PA) is in place for all Participating Organizations; The PA reflects the scope of the information shared.
 - 5.4.2 For Patient Requests: N/A.
- 5.5 How is the shared information secured by the recipient?
 - 5.5.1 For Authorized Users: The PA requires Participating Organization to implement the technical safeguards required by HIPAA Security Rule (45 C.F.R. Part 164).
 - 5.5.2 For Patient Requests: N/A
- 5.6 What type of training is required for users from organizations outside HealthConnections prior to receiving access to the information?
 - 5.6.1 For Authorized Users: The RHIO Administrator receives training regarding their responsibilities. The training materials are located on our website: <https://www.healthconnections.org/resources/training-documents/>.
 - 5.6.2 For Patient Requests: N/A.

Section 6.0

Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

- 6.1 Was notice provided to the individual prior to the collection of information?
 - 6.1.1 Yes, HealthConnections has its [Privacy Policy](https://www.healthconnections.org/resources/privacy-policy/) posted on the bottom of each webpage, including the webpages that have the Authorized User forms (<https://www.healthconnections.org/resources/training-documents/>) and Patient Request forms (<https://www.healthconnections.org/resources/for-patients/>).
- 6.2 Do individuals have the opportunity and/or right to decline to provide information?
 - 6.2.1 The individual can decline to provide such information; in this case, HealthConnections will not be able to respond to the request or complaint.
- 6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
 - 6.3.1 Individuals' rights are described in our Privacy Policy <https://www.healthconnections.org/privacy-policy/>

Section 7.0

Individual Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

- 7.1 What are the procedures that allow individuals to gain access to their own information?
 - 7.1.1 The individual may gain access to their own information by contacting our Support Team at 315.671.2241 x5, using the Contact Us feature on our website (<https://www.healthconnections.org/contact-us/>).
- 7.2 What are the procedures for correcting inaccurate or erroneous information?
 - 7.2.1 The individual can contact us by email at compliance@healthconnections.org, or by referring to the contact details at the bottom of our Privacy Policy <https://www.healthconnections.org/privacy-policy/>
- 7.3 How are individuals notified of the procedures for correcting their information?
 - 7.3.1 These procedures are described in our Privacy Policy <https://www.healthconnections.org/privacy-policy/>
- 7.4 If no formal redress is provided, what alternatives are available to the individual?
 - 7.4.1 N/A

Section 8.0

Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

8.1.1 Basic Users have access to our ticketing system.

8.2 Will contractors to HealthConnections have access to the system?

8.2.1 HealthConnections' contractors may have access to the system if they are responsible for responding to patient-related requests.

8.3 Does the system use "roles" to assign privileges to users of the system?

8.3.1 Yes, the system has role-based access.

8.4 What procedures are in place to determine which users may access the system and are they documented?

8.4.1 HealthConnections assigns roles based on users' duties and responsibilities as HealthConnections' workforce members.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

8.5.1 Requests for system access go through a formal approval process.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

8.6.1 HealthConnections performs routine audits of provisioned users by comparing users' privileges with users' duties and responsibilities as employees or contractors of HealthConnections. HealthConnections employs multifactor authentication, encryption, monitoring, audit logging, and firewall technologies to prevent the misuse of data.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

8.7.1 HealthConnections' provides annual privacy and security training to all workforce members.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

8.8.1 N/A; HealthConnections is not subject to FISMA. HealthConnections is governed by New York State regulation ([10 NYCRR § 300.3\(b\)\(1\) v4.1](#)) and secures information in accordance with these requirements.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

9

9.1.1 Yes. At system acquisition, HealthConnections performs a review of potential vendors to assess whether their functionality and security meet our requirements.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

9.1.2 HealthConnections requires systems that will handle personally identifiable information to meet specified integrity, privacy, and security requirements. Providers of such systems are required to hold certain security certifications and/or complete a security questionnaire. Review of security certifications and/or questionnaire responses are used to evaluate whether the system is adequately designed. Our ticketing system meets our integrity, privacy, and security requirements.

9.3 What design choices were made to enhance privacy?

9.1.3 HealthConnections has implemented encryption, monitoring, and audit logging to enhance privacy.

Conclusion

HealthConnections constructed its system in compliance with federal and state regulations, based on assessing privacy risks and implementing appropriate risk mitigation strategies.

Questions? Contact Us.

Contact us by email at compliance@healthconnections.org, use the [Contact Us](#) feature on our website, or by telephoning our Support Team at 315.671.2241 x5

Approval Page

Liana Prosonic, Privacy Officer

Revision History

Date	Notes	Approved by
11/21/2023	Document Creation	Liana Prosonic
11/21/2024	Annual Review	Liana Prosonic
11/21/2025	Annual Review	Liana Prosonic