



Privacy Impact Assessment (PIA) - HealthConnections Portal

Introduction

This Privacy Impact Assessment (PIA) evaluates the privacy risks and mitigation strategies for HealthConnections Portal, which handles Personally Identifiable Information (PII). The assessment facilitates compliance with applicable regulations, such as HIPAA, and promotes responsible data management practices.

Purpose of the Assessment

The purpose of this assessment is to identify potential privacy concerns related to the collection, storage, processing, and transmission of personally identifiable information (PII) within the software, and to recommend safeguards that protect individuals' sensitive data from unauthorized access, disclosure, or misuse.

Section 1.0 The System and the Information Stored within the System.

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

What information may be stored?

Patients: Information about you as a patient comes from our Participants that have provided you with health care, health insurance, or social supports. The following may be stored in the system: Patient health records, including diagnoses, test results, medications, treatment and other information; health related social needs data, including housing, transportation, food insecurity and other social needs; demographic information including your name, sex, date of birth, insurance information, and other unique identifiers. HealthConnections stores information received by its Participants as a Business Associate to those Participants. HealthConnections does not have control over the information that is transmitted to us; we hold the information in accordance with agreements with those Participants. HealthConnections limits the amount of personally identifiable information in our audit logs to a system-generated unique identifier "target person id" which is the minimum personally identifiable information relevant to our audit logging. We do not record identifiers such as your social security number, date of birth, address, or driver's license in our audit logs.

Authorized Users: Information about you, if you are an authorized user of our portal, is limited to your user name, user id, your role, and organization(s) with which you are affiliated, which is the minimum personally identifiable information relevant to our audit logging.

Why is the information being collected?

Patients: Data is collected by our Participants based on their own policies, procedures and legal requirements. This information is collected by our Participants in the course of



providing services, including but not limited to health care, care-coordination, and social services. These may include hospitals, physicians, pharmacies, clinical laboratories, health insurers, the Medicaid program, community-based organizations, and other organizations that exchange health or social needs information electronically. A complete, current list is available on our website here: [Data Contributors - HealthConnections](#).

Authorized Users: Data is collected in our ticketing system so that HeC can verify your identity and right of access.

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.

Describe all uses of the information.

1. Data may be accessed and used by HealthConnections and our Participants in accordance with applicable regulations. The following uses by Participants require your consent: treatment, insurance eligibility verification, case management activities, quality improvement activities; utilization review.
2. In addition, certain Participants that provide urgent medical care may access your information if they are treating you for a medical emergency, unless you have previously denied consent for that Participant or denied consent for all Participants.
3. Federal, state or local public health agencies, death investigators, and certain organ procurement organizations are authorized by law to access health information without your consent for certain purposes such as death investigations, public health and organ harvesting; these entities may access your information through HealthConnections for these purposes without regard to whether you give consent, deny consent or do not fill out a consent form.
4. HealthConnections may access data without consent for operational purposes, such as system testing, data validation, and required statistical reporting.
5. HealthConnections may access your data to respond to your request or inquiry, such as if you request a copy of your records or if you request a copy of our audit logs showing which Participants have accessed your data.
6. User identifying information is used to authenticate your identity and log your activities within the system.

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

HealthConnections does not mine data but does provide Participants with analytical tools and reports that focus on examining, cleaning, transforming, and modeling data to extract meaningful insights that support decision-making and often involves data visualization to communicate findings. Examples include: A report that provides a



Participant with a list of their patients with hypertension; A graph showing the percentage of a Participant's patients with diabetes who have high A1C levels.

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

1. HealthConnections Portal does not collect information from individuals; however, it does contain information about individuals collected by our Participants or our ticketing system.
2. HealthConnections uses certain tools to ensure that patient records received by various Participants are aggregated appropriately by analyzing demographic information; this includes ensuring that records for two different individuals with the same name are separated and attributed to the correct individuals, while also ensuring that records from the same individual with two different names (e.g., a maiden name) are matched together. This process is large completed by a computer algorithm, with a manual review of records that do not meet the established threshold for automatic matching or segregation.
3. In addition, HealthConnections reviews data feeds to ensure that data received is mapped appropriately, such as verifying whether certain date field is the visit date or a date of birth.
4. HealthConnections does not have the authority to update or change the underlying records received by a Participant. HealthConnections only has control over the aggregation and mapping of such data. When HealthConnections becomes aware of an aggregation or mapping issue, HealthConnections will lock the patient record(s) until the issue is resolved to ensure erroneous information is not accessible to users.
5. When HealthConnections becomes aware of an error or suspected error in the underlying records received by a Participant, HealthConnections will contact the Participant so they can investigate and correct the error, if applicable.
6. With respect to authorized users, HealthConnections requires your organization's RHIO Administrator (our main contact) to validate your identity and role to prevent unauthorized access.

Section 3.0 Retention

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

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

The software must be able to store audit logs for a minimum of six years, per federal regulations.

Patients: HealthConnections does not have an obligation to retain records received by Participants, since the data we hold is a copy of the data they maintain in their own system; such Participants may be subject to regulations requiring them to hold the



original records. Questions regarding any Participant's record retention policy will be directed to that Participant. HealthConnections maintains clinical records for a minimum of 6 years of records per our internal policy; older data may occasionally be archived or deleted.

Authorized Users: HealthConnections maintains authorized users' data for a minimum of 6 years to be able to identify such users in the audit logs.

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

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



Section 4.0 Internal Sharing and Disclosure

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

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

HealthConnections does not have any subsidiary or affiliate organizations.

HealthConnections workforce members who have received training and signed our acceptable use policy and non-disclosure agreement have access to the information.

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

HealthConnections does not have any subsidiary or affiliate organizations.

HealthConnections workforce members may access all information for the following purposes:

1. For the conversion of paper patient medical records into electronic form or for the uploading of Protected Health Information from the records of a Data Supplier provided that HealthConnections is serving as the Data Supplier's Business Associate and (ii) we do not Disclose the information until Affirmative Consent is obtained, except as otherwise permitted by law or regulation.
2. To enable the QE to perform system maintenance, testing and troubleshooting, and to provide similar operational and technical support.
3. At the request of a Participant in order to assist the Participant in carrying out activities for which the Participant has obtained the patient's Affirmative Consent.
4. For the purpose of evaluating and improving our operations.
5. To audit user activities.

How is the information transmitted or disclosed?

HealthConnections workforce members access the information by logging into the system. HealthConnections may access data without consent for operational purposes, such as system testing, data validation, and required auditing and statistical reporting.

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.

With which external organization(s) is the information shared?

1. HealthConnections Participants may access or receive patient information in accordance with agreements between the Participant and HealthConnections, and in accordance with applicable laws, regulations, and policies. A complete list of Participants may be found here: [HealthConnections - Map](#). Participants may direct us to transmit this information to their Business Associates, such as their electronic health records system.
2. Certain HealthConnections' vendors access patient or authorized user information in accordance with agreements between the vendor and HealthConnections, and in accordance with applicable laws, regulations, and policies.

What information is shared and for what purpose?

1. Certain participants' users may only have access to demographic information, while other users will have access to clinical and demographic information based on their role. Roles are assigned and authorized by the Participant.
2. Participants' users may access or receive patient information based on their role and organization type.
 - a. Organ Procurement Organizations and Public Health departments may access all data except for mental health data and substance use disorder data contributed by a "Part 2 Provider" (Part 2 Providers include those who specialize in providing substance use disorder treatment, such as a rehabilitation program, and receive federal funds or are licensed to prescribe controlled substances). This information may be accessed without consent, for permitted purposes, such as monitoring disease trends by Public Health departments or organ harvesting by Organ Procurement Organizations.
 - i. If the public health department is the New York State Office of Mental Health (OMH) or a local/county mental health department authorized by OMH, it may also receive mental health information.
 - b. Community Based Organizations may access limited demographic and clinical information with your consent. The type of information they can access depends on the type of service they provide. Examples include but are not limited to:

- i. A meal delivery service may receive notifications that you have been admitted to a hospital, so they know that you will not need a meal delivery that day.
 - ii. A food bank may access information related to certain conditions that require dietary restrictions, such as diabetes or hypertension.
- c. Disaster relief agencies may access limited demographic and facility information, and dates of admission and discharge, during a declared disaster, without consent, for the purpose of locating individuals.
- d. Health Insurers and other payers such as Medicaid may access your records except for substance use disorder data contributed by a “Part 2 Provider” for the purpose of required regulatory reporting of certain quality measures. Payers may also receive alerts regarding your hospital visits unless you have denied consent to that organization.
- e. Providers of emergent care may access all information to treat you during a life-threatening emergency, unless you previously denied consent to that organization.
- f. Certain Participants can subscribe to an alerting service to receive notifications regarding your hospital visits.
 - i. If the hospitalization was at a facility that is subject to New York Mental Hygiene Law, the alert may be transmitted to Participants authorized by the New York State Office of Mental Health, unless you previously denied consent to that Participant.
 - ii. Otherwise, the alert may be transmitted to Participants without consent if the recipient of such Patient Care Alert is a Participant that provides, or is responsible for providing, Treatment or Care Management to you, unless you previously denied consent to that Participant.
- g. Other Participants may access demographic, social needs, and clinical information if you have given your consent, but only for the following purposes: treatment, care management, insurance eligibility verification, quality improvement activities, and utilization review (by health insurers and payers).
- h. Death Notifications may be sent to a Participant that (a) was responsible for providing Treatment or Care Management to such patient prior to the patient’s death; or (b) is a Payer Organization that provided health coverage to the patient immediately prior to the patient’s death. A death notification may only include Demographic Information and the date and time of death.

- i. Limited or deidentified data may be shared with researchers without consent as long as the request complies with federal and state regulations and we have entered into a data use agreement with the researcher that lists the permitted uses, requirements for confidentiality, prohibitions on redisclosure and prohibits any attempts to re-identify the data. The type of information shared will depend on the nature of the research. Limited and deidentified data are anonymized to exclude your name and other identifiers. HealthConnections does currently support any research projects where Protected Health Information is disclosed.
3. HealthConnections' contractors may access all information without consent when directed by HealthConnections and in compliance with the purposes permitted for HealthConnections' authorized users as detailed in section 4 of this document.
4. Participants may access information regarding their users, to verify their level of access, and review or audit their users activities.

How is the information transmitted or disclosed?

Patients' Protected Health Information may be transmitted to disclosed through any of various secure methods, including:

- By logging on to HealthConnections Portal, our secure health information exchange platform
- By secure file transfer (sFTP)
- By encrypted email communications
- By secure transmission to the Participant or the Participant's Business Associate, such as the Participant's electronic health records system.

Authorized User information, limited to name, username, organization and role, may be communicated through email or by viewing audit log reports.

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?

Information may be shared with external organizations, provided agreements are in place:

1. A Participation Agreement (PA) is in place for all Participating Organizations; The PA reflects the scope of the information shared.
2. A Data Use Agreement (DUA) is in place for all research requests. The DUA establishes the scope and permitted uses of the data by the recipient.
3. An agreement is in place with all vendors with access to confidential information.

How is the shared information secured by the recipient?

1. For Personally Identifiable Information (PII):

- a. The PA and/or DUA agreement requires Participating Organizations to implement the technical safeguards required by HIPAA Security Rule (45 C.F.R. Part 164).
 - b. Contractors with access to PII are required to secure PII subject to the Business Associate Agreement and/or Data Security Addendum in place with the contractor. Contractors/vendors undergo a security review as part of the vendor management process, to ensure confidential information is protected.
2. For anonymized data used in research: Security and confidentiality requirements are incorporated into the agreement.

What type of training is required for users from organizations outside HealthConnections prior to receiving access to the information?

1. For Participants: The RHIO Administrator receives training regarding their responsibilities. The training materials are located on our website: <https://www.healthconnections.org/resources/training-documents/>.
2. For HealthConnections' contractors: All contractors who have access to Personally Identifiable Information are required to receive privacy and security training.

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.

Was notice provided to the individual prior to the collection of information?

HealthConnections does not collect information from individuals in the HealthConnections Portal.

- HealthConnections hold patient information as a Business Associate of Participants. Participants are responsible for providing this notice.
- Authorized users apply through our website, which has a link to our privacy policy at the bottom of the website.

Do individuals have the opportunity and/or right to decline to provide information?

HealthConnections does not collect information from individuals in the HealthConnections Portal.

- Patients: HealthConnections hold this information as a Business Associate of Participants. Participants are responsible for giving individuals the opportunity to decline to provide information, or for complying with their right to decline to provide information.
- Authorized Users: HealthConnections cannot create an authorized user's account if the individual refuses to provide their personal information.

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Patients: In general, individuals have the right to consent or deny consent for Participants to their information. However, in certain circumstances, individuals do not have the right to deny consent to uses of their information. Such circumstances are described above and are summarized here:

- When used by a public health department for permitted purposes
- When used by an organ procurement organization for permitted purposes
- When used by a death investigator for permitted purposes
- When used by HealtheConnections to deliver death notifications
- When used by Disaster Relief Agencies for locating individuals
- When used by HealtheConnections and its contractors for permitted operational purposes and
- When used by HealtheConnections to upload records from Data Suppliers to the HealtheConnections Portal

Authorized Users: Authorized users cannot withhold consent to the use of their information. Collection of user information is required by law.

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.

What are the procedures that allow individuals to gain access to their own information?

Patients may gain access to their own information by either contacting our Support Team at 315.671.2241 x5 or downloading a patient medical record request or audit log request form from our website. [Resources - HealtheConnections](#)

Authorized users gain access to their own information by contacting HealtheConnections by email Support@healtheconnections.org, phone 315-671-2241 ext. 5, or by using the Contact Us feature: [Contact Us - HealtheConnections](#);

What are the procedures for correcting inaccurate or erroneous information?

1. If a patient discovers an error in the aggregation or mapping of the data, they should notify HealtheConnections by email Support@healtheconnections.org, phone 315-671-2241 ext. 5, or by using the Contact Us feature: [Contact Us - HealtheConnections](#).
2. If the patient suspects there is an error in the underlying records that were contributed by a Participant, they should contact that Participant. Participant information can be found here: [HealtheConnections - Map](#).
 - a. If the patient contacts HealtheConnections, HealtheConnections will point them to the correct Participant so that the records can be corrected.
3. If an authorized user discovers an error in their data, they should notify HealtheConnections by email Support@healtheconnections.org, phone 315-671-2241 ext. 5, or by using the Contact Us feature: [Contact Us - HealtheConnections](#); alternatively, they can contact the RHIO Administrator at their organization to request their data be updated – the RHIO Administrator will need to contact HealtheConnections to update the data.

Section 8.0 Technical Access and Security

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

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

Workforce members have access to the system after confidentiality agreements are signed and privacy and security training is completed.

Will contractors to HealthConnections have access to the system?

HealthConnections grants access to certain contractors who provide services that require such access. Examples include, but are not limited to, contractors who provide: technical support, participant support, system design services, system testing services, or infrastructure tools.

Does the system use “roles” to assign privileges to users of the system?

Yes, the system has role-based access.

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

HealthConnections and its Participants' RHIO Administrators are required to review users' duties and responsibilities and assign minimum permissions necessary to perform their tasks, thereby reducing the risk of unauthorized access and potential damage.

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

Requests for system access go through a formal approval process.

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

HealthConnections performs annual audits of authorized users by comparing users' privileges with users' duties and responsibilities as Authorized Users of the system; similarly, HealthConnections' Participants' Audit Contacts perform audits of users approved by their RHIO Administrator. The HealthConnections Portal employs multifactor authentication, encryption, monitoring, audit logging, and firewall technologies to prevent the misuse of data.

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

HealthConnections provides annual privacy and security training for its authorized users, including HIPAA training. Participants' authorized users are required to review and comply with HealthConnections' Privacy and Security Policies and Procedures. New users must attest to receipt of these procedures. Participants' authorized users also undergo annual refresher training.

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

N/A; HealtheConnections is not subject to FISMA. HealtheConnections is governed by New York State regulation ([10 NYCRR § 300.3\(b\)\(1\) v4.1](#)) and undergoes security certifications 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.

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

Yes. HealtheConnections evaluated various technologies when designing the system. The system incorporates solutions from various vendors to leverage the strengths of each vendor/technology.

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

The HealtheConnections Portal was initially developed by a third party. HealtheConnections performed internal testing, review, and analysis to ensure that system requirements were met. HealtheConnections tested role-based access, data tagging (for example, to be able to restrict access to sensitive data, data integrity, among others). In addition, HealtheConnections contracted with several different entities to perform security testing and/or reviews of the system to ensure the system met our integrity, privacy, and security requirements. Examples of such testing and reviews include: code reviews, internal penetration test, external penetration test, web application penetration test.

What design choices were made to enhance privacy?

HealtheConnections has implemented role-based access, data tagging, encryption, monitoring, and audit logging to enhance privacy within the HealtheConnections Portal.

Conclusion

HealtheConnections 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 and Signature Page

Liana Prosonic

Liana Prosonic, Privacy Officer

Revision History

Date	Notes	Approved by
1/14/2025	Document creation	Liana Prosonic, Privacy Officer