Consumer Privacy Policy

Healthcare organizations, who access information sent from MiHIN, are subject to strict confidentiality and accountability standards under the Health Insurance Portability and Accountability Act (HIPAA). In addition, all organizations connected to MiHIN have signed comprehensive data sharing and trust agreements to provide greater protection of information shared. The services currently provided by MiHIN fall into three general categories with regard to health information access, with more specific instances of sharing covered under our Use Case Exhibits:

1. Longitudinal Health Record (LHR) or Virtual Integrated Patient Record (VIPR). The LHR allows your health care providers to search for your health information at the point of care and provides a consolidated view of your health history. MiHIN routinely monitors access of these health records for inappropriate activity.

2. Notifications, Delivery of Results, and Public Health Information.

- Notifications. (E.g. Admissions, Discharge, and Transfer (ADT)) Your healthcare and insurance providers receive a real-time update when you are admitted or discharged from an in-patient setting such as a hospital.

- Results. Your results, which could include but is not limited to laboratory results, radiology results, and transcribed documents, are delivered to health care providers electronically, rather than by a fax machine. This offers a more secure, reliable, and efficient method of delivery. MiHIN delivers health information to health care and insurance providers based on a pre-established Treatment or Payment relationship with patients using our Active Care Relationship Service (ACRS). For example, the Ordering Provider or Primary Care Provider identified on a lab result will receive a copy of the result.

- Public Health. The State of Michigan requires that health information meeting certain criteria be sent to them to monitor the public health of Michigan residents. Similar to email, select pieces of health information can be pushed directly from one health care provider to another. These solutions were also primarily designed as a replacement for fax technology.

3. Direct 'Push' Delivery. Similar to email, select pieces of health information can be pushed directly from one health care provider to another. These solutions were also primarily designed as a replacement for fax technology.

Changing your participation (opting out) with MiHIN affects the availability of your health information within the Longitudinal Health Record only. If you choose to opt-out, information is no longer available to any of your health care providers searching for your information. So, the information will not be deleted, but it will be hidden from providers.

The electronic delivery of your health information in the last two categories may only be restricted by contacting your healthcare provider. Providers are the best resource for opting patients out of health information exchange because they are able to verify the identity of the patient when the request is given, and further, to ensure they are not continuing to send that patient's information to MiHIN against an individual's wishes. Under our legal

agreements and associated Business Associate Agreements (BAAs) with entities, they agree they will not send us information unless they have the appropriate consent or authorization in place necessary. For information shared for Treatment, Payment, and Healthcare operations, an entity may be able to share without consent so long as the individual has not requested their information not be shared. For information that requires consent, such as specially protected information (SPI), the entity should not share with MiHIN unless they obtain the proper consent. An example of this would be substance use disorder information from a federally protected 42 CFR Part 2 facility.

Opt Out Form Update

Frequently Asked Questions:

Under what authority is MiHIN able to share health information for Michigan Residents?
Under the HIPAA Privacy Rule, Covered Entities and Business Associates are able to share information about patients that they have in common for specific purposes. Those are for the purposes of treatment, payment, or healthcare operations. It also allows sharing for public health purposes, though this is subject to slightly different rules under HIPAA.

What are Covered Entities and Business Associates.
Covered Entities are typically organizations who would have direct interactions with patients and are the creators of that patient's information itself. Think of covered entities as providers like your primary care doctor, the hospital that you might visit, or even the entity that pays for your healthcare, like your health insurance plan. Business Associates are entities that support covered entities for the purposes stated above. Think of business associates as an entity's vendors, accountants, lawyers, etc. MiHIN is an example of a business associate and most of our Participant Organizations connected to us are Covered Entities.

Am I able to opt out of health information exchange through MiHIN?
In order to view our entire opt out policy, please scroll up to read our Consumer Privacy Policy. MiHIN facilitates opt out of health information exchange directly with patients in limited situations. We allow opt out of our community health record, which is oftentimes referred to as Longitudinal Health Record (LHR) or Virtual Integrated Patient Record (VIPR).

How am I able to opt out of my LHR/VIPR?
You must complete the standard form listed on this page in order to opt out. This requires filling out limited pieces of demographic information so we can appropriately locate your record. It also requires utilizing a notary, so we are able to confirm you are who you say you are.

What does opt out mean?
Opt out for us means that when a provider searches for the patient in LHR/VIPR, they will not be able to see any health information on that patient. It would be similar to viewing a blank screen. What opt out does not mean is that all information will be deleted.

What if I want to opt out of all health information exchange?

The best way to opt out of all information exchange is to work with your providers to opt out. There are two reasons for this. First, they are able to verify your identity and second, it your provider may have a process for opting out at their organization so information never travels to MiHIN. This protects your privacy by going to the source of information. In addition, in our legal agreements, providers attest they will not share any information that they are not allowed to share by law. Once you are opted out, we can always coordinate with your provider to ensure that your records are no longer being sent to us.

Language for PO Notice of Privacy Practices (NPP):

This organization records and transmits health information electronically through the statewide health information network, Michigan Health Information Network Shared Services (MiHIN). MiHIN coordinates the sharing of information for treatment, payment, healthcare operations, and public health purposes specifically covered under HIPAA. For more information about MiHIN and your rights associated with your information, please refer to their Privacy Policy at https://mihin.org/privacy-policy-for-michigan-health-information-network-shared-services or contact privacy@mihin.org.

Accidental Sharing of Healthcare Information

- Participant Organizations should have their own processes for opting patients out
- Participant organizations should have a process for communicating opt out preferences to us if appropriate
    - Technical component- can we perform an opt out
    - Identity verification piece
    - Practical piece- are individuals aware of HIEs/HINs or more interaction with Provider/ Payer
- All entities who receive information have signed our Business Associate Agreement (BAA), which requires organizations and their workforce members to be trained on access to information and privacy principles such as minimum use.
- Individuals should not access files for patients for whom they do not have an active care relationship.
- When there has been accidental sharing in the past:
    - We have been able to identify accidental sharing through quality process
    - Participant Organizations have also had an open dialogue with us if they believe information has been shared inappropriately
    - We have been able to identify how the accidental sharing occurred through an internal root cause analysis (RCA)
    - We have determined which entities received information on a patient who opted out of exchange
    - We have facilitated the process of coordinating with privacy officials at the receiving organizations to ensure that the information is removed from their system and determine the extent of access to that file (if it occurred)
    - We have facilitated with the sending organization to remind them an opt out has occurred, and determined how to prevent the improper sharing of information in the future
    - We have worked with organizations to communicate to individuals if necessary
        - This communication typically comes from PO

Specially Protected Information (SPI), PO Responsibilities, and More.
An Examination of QDSOA Language.

Entities should not share SPI for which they do not have the proper consent or authorization.

QDSOA Language:

3.2. Compliance in Using, Disclosing and Obtaining Information. PO acknowledges that the information it may provide to or obtain from other Parties through the HIN Services may include PHI, which is subject to protections or limitations on its use or disclosure under federal or state laws. HIN and PO are each separately responsible for ensuring that it complies with Applicable Laws and Standards and the applicable Use Case in sending, receiving, finding, or using information using the HIN Services. **To the extent required by Applicable Laws and Standards, PO shall, or shall require its PO Participants to, obtain any authorization or consent necessary from any individual whose PHI it sends, receives, finds, or uses through the HIN Services.** In the event PO is a Covered Entity as defined under HIPAA, PO is responsible for obtaining any required authorization or consent from any individual whose PHI it sends, receives, finds, or uses through the HIN Services. In the event PO provides access to Consumer Users, PO is responsible for allowing access only as indicated by such Consumer User for any health information it sends, receives, finds, or uses through the HIN Services. With respect to those activities involving the use or disclosure of PHI, the Parties shall comply with the HIPAA Addendum attached hereto as Attachment D. In addition to those requirements under Attachment D, in the event PO sends or receives Message Content for which PO is not authorized to send or receive, PO will immediately inform HIN, delete such Message Content, and require its PO Participants to do so.

8.1.9. Patient Consent. PO agrees that when it sends, receives, finds, or uses Message Content PO will practice consent management and comply with Applicable Laws and Standards. This process enables all parties to determine what Patient Data can be accessed at various points of care. By way of example, if an Exhibit specifies sending Health Information that may not be sent without patient consent under HIPAA or SAMHSA rules, PO must not send any Message Content or Patient Data containing Health Information for which an express patient authorization or consent is required (e.g., mental or behavioral Health Information) without first confirming that a valid patient consent exists and permits Patient Data to be sent only to the receiving Health Provider(s) named by the patient on the consent.

8.1.14. Privacy Tags If required by the HIN Board, the sender of any Message Content that contains Specially Protected Information must include special machine-readable Privacy Tags in the Message Content as specified in the Use Case Implementation Guide. If Message Content contains any Privacy Tags, the sending PO must confirm that patient has consented to recipient receiving the Message Content before PO sends the Message Content.

2.12. HIN will not make any communications to individuals in violation of the restrictions on marketing in HITECH Act § 13406(a) and without the prior consent of PO.

4. Obligations of PO.

4.1. PO shall notify HIN of any limitation(s) in the notice of privacy practices of PO in accordance with 45 CFR § 164.520, to the extent that such limitation may affect HIN's use or disclosure of PHI. HIN will give timely effect to such limitations.

4.2. PO shall notify HIN of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect HIN's use or disclosure of PHI. HIN will give timely effect to such changes or revocations.

4.3. PO shall notify HIN of any restriction to the use or disclosure of PHI that PO has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect HIN's use or disclosure of PHI. HIN will give timely effect to such restrictions.

4.4. PO shall not request HIN to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by PO, except as specifically allowed by the "Specific Use and Disclosure Provisions" Section of this Addendum.

19. Minimum Necessary Requirements. PO shall satisfy the Minimum Necessary Requirements as if they applied to EHI when its Uses or Discloses EHI for applicable Exchange Purposes or when PO requests EHI in the context of the applicable Framework Agreement. The Minimum Necessary Requirements shall apply to PO regardless of whether it is a Covered Entity or a Business Associate when it requests, Uses, or Disclosures EHI. Any provisions set forth in the HIPAA Rules (e.g., 45 CFR § 164.514 (d)) that include conditions shall also apply to PO when Using, Disclosing, or requesting EHI if such provisions are applicable.

In addition, the Minimum Necessary Requirements do not apply under certain circumstances set forth in the HIPAA Rules including the following: (i) a Disclosure of PHI to or request by a health care provider for Treatment; (ii) a Disclosure to an Individual who is the subject of the information; (iii) a Disclosure pursuant to an Individual's authorization under 45 CFR § 164.508; or (iv) Disclosures that are required by laws as described in 45 CFR § 164.512(a). These exclusions apply to a PO with regard to EHI.