Iowa Health Information Network (IHIN)

PRIVACY POLICIES
April 2017

IHIN Privacy Policies
Change History and Policy Approvals

Change History

Date:	Changes:
07/10/2013	1. Amendment 1- limiting the use of the query/look-up function for treatment purposes only and not payment and operations. Amendment 1 has an expiration date and other caveats for termination and is attached within this document.
07/09/2014	2. Amendment 2 – changes made to the Administrative Safeguards section allows for Direct Secure Messaging to be used for Treatment Payment and Healthcare Operations by all Participants, including commercial health plans.
01/14/2015	1. Revised and updated the definition of HIPAA to include reference to the Omnibus Rule. 2. Throughout the document made edits to allow the Participant to apply equivalent standards of these policies to their BAA's and contractors. 3. Policy 9 is edited to reflect changes to HIPAA which allow a patient to restrict disclosure of information in specific instances.
06/30/2015	Amendment 1 – The Treatment Only period has been terminated with the passage of HF 381 which expands the allowable uses of the record locator service from just Treatment to Treatment, Payment and Healthcare Operations as defined by HIPAA. This amendment and link to HF 381 has been moved to the back of the document for historical reference.
4/1/17	Transition to private entity changes (replacement of references to Department and IDPH with IHIN)

Policy Approvals

Description:	Approved By:	Date:
Original Approval	State Board of Health	11/14/12
Amendment 1	State Board of Health	7/10/13
Amendment 2	State Board of Health	7/09/14
Full review	State Board of Health	01/14/2015
Replacement of references to Department and IDPH with IHIN	IHIN	4/13/17

TABLE OF CONTENTS

INTRODUCTION *4*

DEFINITIONS:..... *7*

IHIN PRIVACY POLICY 1: *COMPLIANCE WITH LAW AND POLICY* *10*

IHIN PRIVACY POLICY 2: *NOTICE OF PRIVACY PRACTICES*..... *11*

IHIN PRIVACY POLICY 3: *INDIVIDUAL CONTROL OF INFORMATION AVAILABLE THROUGH THE IHIN* *12*

IHIN PRIVACY POLICY 4: *ACCESS TO AND USE AND DISCLOSURE OF INFORMATION*..... *16*

IHIN PRIVACY POLICY 5: *INFORMATION SUBJECT TO SPECIAL PROTECTION.* *19*

IHIN PRIVACY POLICY 6: *MINIMUM NECESSARY* *21*

IHIN PRIVACY POLICY 7: *WORKFORCE, AGENTS, AND CONTRACTORS* *22*

IHIN PRIVACY POLICY 8: *AMENDMENT OF DATA* *24*

IHIN PRIVACY POLICY 9: *REQUESTS FOR RESTRICTIONS* *25*

IHIN PRIVACY POLICY 10: *MITIGATION* *26*

IHIN PRIVACY POLICY 11: *BREACH INVESTIGATIONS AND INCIDENT RESPONSE* *28*

IHIN PRIVACY POLICY 12: *AUTHORIZED PERSONNEL AND AUTHORIZED USER CONTROLS*..... *30*

Iowa Health Information Network (IHIN) Privacy Policies

INTRODUCTION

The following policies apply to the access, use and disclosure of Protected Health Information (PHI) by Participants through the IHIN. These Privacy Policies follow the principles of the core domains of the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.[1] The guiding privacy principles are as follows:

Individual Access: Individuals should be provided with a simple and timely means to access and obtain their PHI in a readable form and format.

Correction: Patients must have the ability to dispute the accuracy or integrity of their health data and have erroneous information corrected or to have a dispute documented if their requests are denied.

Openness and Transparency: Individuals should be able to understand what information exists about them, how the information is used, and how they can control use of that information.

Individual Choice: Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their PHI.

Collection, Use and Disclosure Limitation: PHI should be collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose.

Data Quality and Integrity: Participants should take reasonable steps to ensure that PHI is complete, accurate and up-to-date to the extent necessary for the Participant's intended purposes, and has not been altered or destroyed in an unauthorized manner.

Safeguards: PHI should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use or disclosure.

Accountability: Appropriate monitoring mechanisms should be in place to report and mitigate non-adherence to policies and identification of Breaches.

[1] *healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_privacy_security_framework//1173*

EFFECT OF LEGISLATION AND RULE CHANGES. The IHIN and Participants need to remain flexible in approach in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the HITECH Act.[2]

ADMINISTRATIVE SAFEGUARDS FOR REQUESTING PHI. HIPAA permits a covered entity that holds PHI to disclose such information to other covered entities both for purposes of its own, treatment, payment and healthcare operations (TPO), and for the treatment, payment and certain healthcare operations purposes of such other covered entities without patient consent.[3] HIPAA limits authority to disclose without consent in other situations and attaches conditions to such disclosure. HIPAA thus places a duty on Participants exchanging PHI to determine that each proposed disclosure is permitted.

Accordingly, to permit Participants that furnish information to meet their obligation to disclose PHI only for a qualifying purpose, and to meet certain other conditions, the IHIN and Participants place the burden on the requesting Participant to:

- Access information from another Participant's records only for a qualifying TPO use by the requesting Participant. A qualifying TPO use is one that would permit the Participant from whose records the information is accessed to disclose such information to the requesting Participant under §§ 164.506(c)(2), (3), or (4) of the Privacy Rule.

- In connection with access for payment purposes, to access and use only the minimum information necessary for purposes of the payment needs of the Participant accessing the information.

To support this approach, the IHIN and Participants have implemented the following administrative safeguards:

- All Participants may use the IHIN Direct Secure Messaging functionality to exchange PHI for purposes of their TPO.
- Participants that are providers or Iowa Medicaid Enterprise (IME), with respect to its clients, may use the query functionality of the IHIN to access and disclose PHI only for their TPO purposes.
- Commercial health plans and Participants that are acting as plan administrators of health plans covered under HIPAA will not have access to the query functionality of the IHIN until such time that the technology

[2] The Participants acknowledge the need to revise their policies and certain other technical and administrative features to conform to HITECH and regulations to be promulgated hereunder. Participants will make the required changes promptly.
[3] 45 C.F.R. § 164.506(c).

has developed to enable restriction of the results of a query to those encounters, tests, or other treatments which are paid for by the health plan. Once the technical capability is available, this functionality will be tested and presented to the appropriate workgroups, IHIN Advisory Council and Executive Committee for consideration and approval.

DEFINITIONS:

"Authorized Users" means those members of Participant's Workforce (including employees, agents, contractors and any other persons having access to the IHIN by virtue of their relationship with Participant) who are individually authorized by Participant to have access to the IHIN to assist Participant in providing treatment, payment or healthcare operations, as permitted by applicable federal and Iowa law, and to whom Participant has assigned a unique identifier for access to the IHIN.

"Breach" means breach as such term is defined in the Privacy Rule.

"Business Associate" or "BA" means a business associate as such term is defined in the Privacy Rule.

"Business Associate Agreement" or "BAA" means the business associate agreement posted on the IHIN website.

"IHIN's Authorized Personnel" or "Authorized Personnel" means the IHIN's employees, agents and independent contractors who have access to the IHIN for the purposes described in Privacy Policy 4, section 2.2, and who are under obligations substantially similar to the provisions contained in these Privacy Policies.

"HIPAA" means the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act and the regulations promulgated thereunder, including, without limitation, the Privacy Rule, the Security Rule, the Breach Notification Rule, the Enforcement Rule, and the Final Omnibus Rule Modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, as any or all may be amended from time to time.

"HITECH Act" means Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (Feb. 17, 2009), and the regulations promulgated thereunder.

"IHIN" means the Iowa Health Information Network, including all hardware provided, all software used or provided, all written specifications and user and technical manuals provided regarding the functionality and operation of the IHIN, and all data exchange and other services provided through the IHIN.

"Individual" or "individual" means a patient or client of a Participant.

"Other Participants" means other entities that have access to the IHIN and have signed a Participation Agreement containing an obligation to comply with the IHIN Privacy and Security Policies, and to be responsible for any Business Associate, contractor or Workforce member who accesses and uses the IHIN as an Authorized User on its behalf.

"Participant" means an authorized organization that has voluntarily agreed to enter into a Participation Agreement to access or use the IHIN.

"Participant ID" means a unique user identifier assigned to a Participant by the Department. The Participant then issues unique identifiers to each of its Authorized Users.

"Participation Agreement" means the agreement entered into between the IHIN and a Participant that prescribes the terms and conditions for access and use of the IHIN.

"Payer or Health Plan" means, but is not limited to, an insurance company, self-insured employer, government program, individual or other purchaser that makes payments for health services.

"Privacy Policies" and "Security Policies" means the IHIN's rules, regulations, policies, standards and procedures for access to and use of the IHIN, as from time to time posted electronically on the IHIN website or otherwise furnished to Participant.

"Privacy Rule" means the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

"Protected Health Information" or "PHI" means protected health information as defined in 45 C.F.R. § 160.103 that is created or received by an authorized Participant.

"Provider" means a person or organization that is a health care provider under HIPAA and is licensed or otherwise permitted to provide health care items and services under applicable state law.

"Security Rule" means the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. part 160 and subparts A and C of part 164.

"Subcontractor" means any third party engaged by the IHIN to assist in the design, operation, or in the performance of the IHIN's obligations under this Agreement.

"TPO" means treatment, payment, or healthcare operations, as such terms are defined in the Privacy Rule.

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, as defined in the HIPAA Privacy Rule.

IHIN Privacy Policy 1: *Compliance with Law and Policy*

Scope and Applicability: This Policy applies to all Participants.

Policy: Participants shall comply with all applicable laws and these Privacy Policies in accessing and using the IHIN.

Standards:

1. **Laws.** Each Participant shall, at all times, comply with all applicable federal and state laws and regulations, including, but not limited to, those protecting the confidentiality and security of PHI and establishing certain individual privacy rights. Each Participant must use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

2. **IHIN Policies.** Each Participant shall, at all times, comply with these Privacy Policies. These Privacy Policies may be changed and updated by the IHIN upon reasonable written notice to Participants. Amendment(s) shall be effective when approved by the IHIN Executive Committee. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Privacy Policies.

3. **Participant Policies.** Each Participant is responsible for establishing internal policies that are necessary to comply with applicable laws and these Privacy Policies.

4. **Conflicting Policies**. In the event of a conflict between the IHIN's policies and the Participant's policies related to the IHIN, the IHIN's policies related to the IHIN shall control over Participant's policies, unless a Participant policy is more restrictive than the IHIN's policy, in which case the Participant's more restrictive policy will apply to that Participant only.

5. **Participant Criteria.** Each Participant shall be a HIPAA "covered entity" or Business Associate and thus subject to both its individual legal duty as a regulated covered entity under HIPAA and its contractually assumed obligations under the Participation Agreement.

6. **User Criteria.** Each Authorized User derives his or her permission to access and use the IHIN from a Participant. Therefore each Authorized User must maintain a current relationship to a Participant in order to use the IHIN. Authorized Users must therefore be one of the following: (i) Participants (for example, an individual physician) or Workforce of a Participant, (ii) an individual BA or Workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or Workforce of such

contractor or subcontractor. A Participant that is a covered health plan may also be an Authorized User in its role as a third party administrator and BA for self-funded group health plans that are covered entities under HIPAA but are not themselves Participants.

7. **Application to BAs and Contractors.** Participants shall apply this policy or standards equivalent to those in this policy, to their BAs, and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Privacy Policy 2: *Notice of Privacy Practices*

Scope and Applicability: This Policy applies to all Participants.

Policy: Each Participant shall develop, maintain and distribute a Notice of Privacy Practices (NPP) that describes the uses and disclosures of PHI contemplated through the Participant's participation in the IHIN.

Standards:

1. **Content.** The NPP shall meet the content requirements set forth under the Privacy Rule[4] and comply with applicable laws and regulations. Participants shall individually determine whether their current NPP requires amendment to reflect their contemplated use and disclosure of PHI through the IHIN and amend their policies if such use and disclosure is not reflected. The IHIN provides the following sample language for Participants to use in amending their NPP:

   > *"We may make your protected health information available electronically through an electronic health information exchange (HIE). An HIE is a system that facilitates the exchange of electronic health records or other clinical or public health information between its participants. As a participant in an HIE, we may provide your health information to other health care providers and health plans that request your information for their treatment, payment and healthcare operations purposes. Participation in an HIE also permits us to access their information about you for our treatment, payment and healthcare operations purposes."*

2. **Dissemination and Individual Awareness.** Each Participant shall have its own policies and standards governing distribution of the NPP to individuals, and, where applicable, acknowledgment of receipt by the individual.[5] Such policies and standards shall comply with all applicable laws and regulations.

3. **Participant Choice.** Participants may choose a more proactive NPP distribution or patient awareness process than provided herein and may include more detail in their NPP, so long as any expanded detail does not misstate the safeguards supporting the IHIN.

[4] 45 C.F.R. § 164.520(b).
[5] See 45 C.F.R. § 164.520(c)(2)(ii).

IHIN Privacy Policy 3: ***Individual Control of Information Available Through the IHIN***

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Individuals can choose not to have their PHI included in the IHIN.

Standards:

1. **Choice Whether to Have Information Included in the IHIN.** All individuals will have the opportunity to choose not to participate in the IHIN, which is also referred to in these Privacy Policies as decision to "opt out" of the IHIN. Participants agree to comply with an individual's election to opt out and to promptly report the election to the IHIN, as described in these Privacy Policies.

    1.1 Individuals shall be afforded the opportunity to exercise this choice at the time of any service at a Participant that is a health care provider or through a uniform opt-out process.

    1.2 Participants shall communicate an individual's election to opt out of participation in the IHIN to the IHIN in the manner provided by the IHIN; the election will be of system-wide effect once so communicated and processed.

    1.3 The Department will furnish Participants that are health care providers with information about the IHIN for use in explaining participation in the IHIN. The information will also contain a link to the IHIN website where further explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt-out election can be found.

        1.3.1 The information shall explain the system-wide scope of an opt-out decision, the risks to the individual's data privacy and security if the individual participates, the effect and benefits of participation, and the effect and disadvantages of opting out. The information will explain that a Participant's policies continue to govern access, use and disclosure in all other contexts.

        1.3.2 The information shall state that the Participant (and Other Participants) will not withhold coverage or care from an individual on the basis of that individual's choice to opt out of the IHIN.

        1.3.3 Participants will inform individuals about the opportunity to opt out and make the information available to them at the initial episode of care after Participant joins the IHIN and thereafter upon request. Each Participant will have one or more persons designated to answer questions about the

IHIN or about opting out or revoking a prior opt-out election.

1.4 Participants may also direct individuals to the IHIN website and to a help line where the individual can ask additional questions and obtain additional information about participation in the IHIN and opt-out decisions.

1.5 Participant authorizes the IHIN to provide information and answer individual questions about the IHIN and opt-out alternatives on behalf of Participant.

1.6 Participants that are health plans provide only limited enrollment and eligibility information through the IHIN and have limited or no face-to-face contact with individuals. Participants that are health plans shall provide a description of the IHIN to their enrollees, an explanation of the right to opt out, a link to the IHIN website, and telephone number individuals can use to obtain additional information about the IHIN, insurer access, and the right to opt out. This information shall be included in the health plan's annual NPP and otherwise as determined necessary.

2. **Participant's Choice.** Participants shall develop and implement the necessary processes to allow an individual to choose not to have information about him or her included in the IHIN. Participants may employ a consent model different than the IHIN default, and processes will vary based on each Participant's operational and technical capabilities. The consent models and processes described in this Policy are not exhaustive, and Participants may adopt additional, consistent mechanisms. The default is that the available health information of an individual will be included in the IHIN automatically, but the individual will be given the option to opt out of the IHIN completely through a Participant or directly through the IHIN. Other consent models that may be available through a Participant include, by way of example:

2.1 Opt-out with exceptions. Default is for health information of patients to be included automatically, but the patient can opt out completely or selectively exclude categories of data or specific data elements from the exchange (e.g., limit exchange of information to specific providers / provider organizations; limit exchange of information for specific purposes). This option is only available at the Participant level.

2.2 Opt-in. Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out. This option is only available at the Participant level.

2.3 Opt-in with restrictions. Default is that no patient health information is made available, but the patient may allow a subset of select data to be included (e.g., permitting only certain providers involved in their care to access information; provide only

temporary access to the provider during a specified time frame). This option is only available at the Participant level.

Participant shall inform its patients who choose a consent model at the Participant level that such model is specific to that Participant and will not apply to the health information that the patient's other providers may have.

3. **Change to Prior Election.** An individual who has opted out of participation in IHIN can later elect to opt back in. The information provided by the Participant and information on the IHIN website shall inform the individual that withdrawing a prior opt-out election will result in information that was previously unavailable through the IHIN becoming available through the IHIN.

4. **Effect of Choice.** An individual who chooses to opt out of the IHIN opts out as to all of his or her records made available through the IHIN, not just with respect to a particular Participant or episode of care. The effect is system-wide. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use and disclosure occurring before the decision is received and communicated through the IHIN.

5. **Limited Effect of Opt Out.** A decision to opt out only affects the availability of the individual's PHI through the IHIN query functionality. It will not affect the use of the individual's PHI by the individual's providers through the direct secure messaging function of the IHIN unless the Participant has otherwise agreed with the individual. In other words, a point-to-point exchange of data between two Participants that have, have had or are scheduled to have a relationship with the individual can still occur even if a patient has opted out of the IHIN. Each Participant's policies continue to govern access, use, and disclosure in all other contexts and via all other media.

6. **Documentation.** Each Participant shall maintain documentation regarding the procedures it uses to inform individuals about the IHIN and about the ability to opt out of the IHIN.

7. **Provision of Coverage or Care.** A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.

8. **Reliance.** Participants will be entitled to assume that an individual has not opted out if the individual's PHI is available through the IHIN.

9. **Timeliness of Choice**. An election to opt out or to opt back in to the IHIN will be reflected by the IHIN within 3 business days from the IHIN's

receipt of the election or change in election. An election or change in election will not affect information that has been previously exchanged through the IHIN (i.e., once disclosed, information cannot be pulled back). The IHIN will provide a toll-free number for individuals to check the status of an election.

IHIN Privacy Policy 4: *Access to and Use and Disclosure of Information*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Participants shall access, use and disclose PHI through the IHIN only in a manner consistent with all applicable federal and state laws and regulations and not for any unlawful or discriminatory purpose.

Standards:

1. **Documentation and Reliance.** If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing PHI for a particular purpose, the requesting Participant shall ensure that it has obtained the required documentation or met the requisite conditions. Each access and use of PHI by a Participant is a representation to every other Participant whose PHI is being accessed and used that all prerequisites under state and federal law for such disclosure by the disclosing Participant have been met.

2. **Purposes.**

   2.1 A Participant may request and use PHI through the IHIN only for the Participant's TPO and only to the extent necessary and permitted by applicable federal and state laws and regulations, the Participation Agreement, the Security Policies and these Privacy Policies.[6] A Participant may request and use PHI through the IHIN only if the Participant has, has had, or is scheduled to have the requisite relationship to the individual whose PHI is being accessed and used.

3. **Minimum Necessary.** Participant uses, disclosures of, and requests for PHI through the IHIN for purposes other than treatment shall comply with the minimum necessary standard of the Privacy Rule[7] and these Privacy Policies.

4. **Participant Policies.** Each Participant shall reference and maintain compliance with its own internal policies and procedures regarding disclosures of PHI and the conditions that shall be met and documentation that must be obtained, if any, prior to making such disclosures.

5. **Subsequent Use and Disclosure.** A Participant that has accessed PHI through the IHIN and merged the PHI into its own record shall treat the merged information as part of its own record and thereafter use and

[6] 45 C.F.R. § 164.502(a), (b).
[7] 45 C.F.R. § 164.502(b).00

disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participant shall not access PHI through the IHIN for the purpose of disclosing that information to third parties other than for the Participant's qualifying TPO.

6. **Accounting of Disclosures.** Each Participant shall be responsible to account only for its own requests and disclosures. Participants shall access and use the IHIN for treatment, payment and healthcare operations purposes only as follows: (i) each request by a Participant that is a provider is deemed to be for such Participant's treatment, payment or health care operations purposes, (ii) each request by a Participant that is a health plan is deemed to be for such Participant's payment purposes, and (iii) each request by a Participant that is acting as a plan administrator of one or more other health plans covered by HIPAA is deemed to be for the payment purposes of such other health plans.

7. **Audit Logs.** Participant and the IHIN shall develop and have in place prior to use of the IHIN an audit log capability to document Participant's posted and accessed PHI about an individual through the IHIN and when such information was posted and accessed.[8]

8. **Authentication.** The IHIN shall establish an entity authentication process for verifying and authenticating the identity and authority of each Participant.[9] Participant shall provide the individual authentication process for verifying the identity of its Authorized Users.[10] Participants shall be entitled to rely on the IHIN's user access and authorization safeguards and may assume an Authorized User making a request for PHI on behalf of a Participant is authorized to do so. See Privacy Policy 12 for additional details on Authorized User Controls.

9. **Access.** Each Participant should have a formal process through which it permits individuals to view information about them that has been made available by the Participant to the IHIN.[11] Participants and the IHIN will consider and work toward providing patients direct access to the information about them contained in the IHIN.

10. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

[8] See C.F.R. §§ 164.316, 164.308(a)(1)(i).
[9] See 45 C.F.R. §§ 164.514(h), 164.312(d).
[10] See 45 C.F.R. §§ 164.514(h), 164.312(a).
[11] See 45 C.F.R. § 164.524.

11. **Historical Data.** Participants may submit data to IHIN dating as far back as the information is maintained and available on the Participant's information system; there are no historical cut off dates and the extent of historical data provided will vary by Participant.

IHIN Privacy Policy 5: *Information Subject to Special Protection.*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Participants should not make PHI requiring special protection available to the IHIN unless the patient has consented or the disclosure is permitted by law.

Standards:

1. **Special Protection.** The IHIN and these policies are geared to the HIPAA level of privacy. Some health information may be subject to special protection under federal and/or state laws and regulations. Other health information may be deemed so sensitive that a Participant has made special provision to safeguard the information, even if not legally required to do so. Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through the IHIN. A Participant can make PHI requiring special protection available to the IHIN if permitted by law or with the consent of the patient. Each Participant is responsible for complying with laws and regulations and its own policies in regard to identifying and providing special treatment for information needing special protection.

2. **Information Not Furnished.** For IHIN data to be useful, the Participant using it must know if it is complete or whether certain information may have been withheld due to more stringent state and federal law or Participant policies.

   2.1 Accordingly, Participants accessing and using another Participant's information obtained through the IHIN should assume that the information made available would not include any of the following:
   - (a) Alcohol and substance abuse treatment program records;
   - (b) Records of predictive genetic testing performed for genetic counseling purposes;
   - (c) HIV testing information; and
   - (d) Records of mental health treatment centers.

   2.2 This list is suggestive only. Other records may be added to the list. Data recipients are not entitled to rely on records being inclusive of the above listed records.

3. **Application to Business Associates and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have

access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Privacy Policy 6: *Minimum Necessary*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: When requesting health information through the IHIN for purposes other than treatment, each Participant shall request only the minimum amount of health information through the IHIN as is necessary for the intended purpose of the request.

Standards:

1. **Disclosures.** A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs, and with applicable law.

2. **Participant Policies.** Each Participant shall adopt and apply policies to limit access to the IHIN to members of its Workforce who qualify as Authorized Users and only to the extent needed by such Authorized Users to perform their job functions or duties for the Participant.

3. **Application to Health Plans.** A Participant that is a commercial health plan shall use PHI of another Participant only for payment purposes as defined in 42 C.F.R. § 164.501. All payer Participants shall use only the minimum information necessary when using information for payment purposes.

4. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Privacy Policy 7: *Workforce, Agents, and Contractors*

Scope and Applicability: This Policy applies to IHIN and all Participants.

Policy: Participants and the IHIN are responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity or Business Associate under HIPAA and as a Participant in the IHIN, and to train and supervise its Authorized Users and Authorized Personnel to the extent applicable to their job responsibilities.

Standards:

1. **Authorized Access.** The IHIN and Participant will determine who within their organizations will be granted access to the IHIN through their information systems. All Authorized Users, whether members of a Participant's Workforce or member of the Workforce of a BA or contractor, shall complete an Authorized User agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, BA, or contractor, as applicable, these Privacy Policies and the Security Policies. Participants shall determine to what extent members of their Workforce or the Workforce of BAs and contractors require additional training due to the Participant's obligations under their Participation Agreement and these Privacy Policies, and arrange for and document such training. The IHIN shall have the authority in the Participation Agreement to suspend, limit or revoke access authority for violation of applicable law, these Privacy Policies, or the Security Policies.

2. **Access to IHIN.** The IHIN and Participant shall allow access to the IHIN only by those who have a legitimate and appropriate need to use the IHIN and/or release or obtain information through the IHIN. No Workforce member, agent or contractor shall have access to the IHIN except as an Authorized User on behalf of a Participant and subject to the Participant's privacy and security policies and procedures, these Privacy Policies, the Security Policies and the terms of the Authorized User agreement.

3. **Discipline for Non-Compliance.** IHIN and Participant shall establish disciplinary policies to hold Authorized Personnel/Authorized Users, BAs and contractors accountable for failing to follow the Participant's policies and procedures and for ensuring that they do not use, disclose, or request health information except as permitted by these Privacy Policies.[12] Examples of disciplinary measures include, but are not limited to, verbal and written warnings, retraining, demotion, and termination.

[12] See 45 C.F.R. § 164.530(e).

4. **Reporting of Non-Compliance.** Each Participant shall have a procedure, and shall require all Workforce members, BAs and contractors to report any non-compliance with the Participant's policies, these Privacy Policies or the Security Policies applicable to Authorized Users.[13] The IHIN shall have a procedure and shall require its employees, BAs and contractors to report non-compliance with these Privacy Policies or the Security Policies as appropriate. Each Participant also shall establish a mechanism for individuals whose health information is available through the IHIN to report any non-compliance with these Privacy Policies or the Security Policies or concerns about improper disclosures of PHI to Participant.

5. **Enforcing BAs and Contractor Agreements.** Each Participant shall require in any relationship with a BA, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an Authorized User on behalf of the Participant, or that will result in members of the Workforce of such third party becoming an Authorized User on behalf of the Participant, that: (i) such third party and any member of its Workforce shall be subject to these Privacy Policies and the Security Policies when accessing, using or disclosing information through the IHIN and (ii) that such third parties and/or Authorized Users on its Workforce may have their access to the IHIN suspended or terminated for violation of these Privacy Policies, the Security Policies, or other terms and conditions of the Authorized User agreement.

[13] See 45 C.F.R. § 164.530(a), (d).

IHIN Privacy Policy 8: *Amendment of Health Information*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Each Participant shall comply with applicable federal and state laws and regulations regarding individual rights to request amendment of health information.[14]

Standards:

1. **Notification regarding Amended Information.** If an individual requests, and the Participant accepts, an amendment to the health information it has created about the individual, and if the Participant believes that serious health consequences could occur if Other Participants who have accessed the pre-amended health information do not have the amended information, the Participant may choose to notify the IHIN using a method established for such purpose. The Participant, assisted by the IHIN, shall make reasonable efforts, within a reasonable time, to inform Other Participants that accessed or received such information through the IHIN. If one Participant believes there is a medically significant error in the record of another Participant, it shall contact the Other Participant.

2. **Amendment to Merged Information.** If a Participant has merged PHI accessed through the IHIN into its own record and receives a request from the individual who is the subject of the PHI for an amendment to the merged information, the Participant will make a record that the amendment was requested. If the Participant believes there is an error in the merged record that could result in serious health consequences, the Participant shall notify the IHIN and the Participant that created the record.

3. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

[14] See 45 C.F.R. § 164.526.

IHIN Privacy Policy 9: *Requests for Restrictions*

Scope and Applicability: This Policy applies to all Participants.

Policy: Participants who agree to a request for restrictions from an individual should not make the information available through IHIN.

Standards:

1. **Recipient Responsibility.** When accessing health information as a recipient, a Participant shall not be expected to know of or comply with a restriction on use or disclosure agreed to by the Participant providing the health information.

2. **Data Provider Responsibility.** If a Participant agrees to an individual's request for restrictions as permitted under the Privacy Rule,[15] such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the IHIN if required by the restriction. Participants should advise individuals that opting out of participating in the IHIN only affects access, use and disclosure of their PHI through the IHIN. When evaluating a request for a restriction, the Participant shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through the IHIN.

[15] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual.

IHIN Privacy Policy 10: *Mitigation*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: Participants and the IHIN shall mitigate the harmful effects of privacy Breaches occurring through the IHIN.

Standards:

1. **Duty to Mitigate.**

    1.1 The IHIN shall implement a process to mitigate the harmful effects that are known to the IHIN of an access, use, or disclosure of PHI through the IHIN that is in violation of applicable laws and/or regulations and/or these Privacy Policies or the Security Policies, and that is caused or contributed to by IHIN Authorized Personnel. The IHIN shall mitigate, to the extent practicable, any harmful effects that are known to IHIN of a Breach Event. Steps to mitigate may include, but are not limited to, notifying the affected Participant(s) as soon as practicable, but no later than seven (7) days.

    1.2 Participant shall implement a process to mitigate the harmful effects that are known to the Participant of an access, use, or disclosure of PHI through the IHIN that is in violation of applicable laws and/or regulations and/or these Privacy Policies or the Security Policies, and that is caused or contributed to by the Participant or its Workforce members, agents and contractors. Participants shall then mitigate the harmful effects to the extent practicable. Steps to mitigate may include, but are not limited to; (1) Participant notification to the individual; or (2) Participant request to the party who improperly received such information to return and/or destroy the impermissibly disclosed information.

2. **Duty to Cooperate.** A Participant that has caused or contributed to a privacy Breach or that could assist with mitigation of the effects of such Breach shall cooperate with the IHIN by taking reasonable steps to help mitigate the harmful effects of the Breach. A Participant shall be deemed to have caused or contributed to a privacy Breach if its BA or agent acting on behalf of the Participant caused or contributed to the privacy breach. A Participant that has not caused or contributed to a privacy Breach (and its BAs and agents did not cause or contribute to the privacy Breach) but nonetheless could assist with the mitigation of the effects of such Breach may assist in the mitigation if asked and if practicable to do so.

3. **Notification to the IHIN.** A Participant that has caused or contributed to a privacy Breach shall notify the IHIN of all events requiring mitigation and of all actions taken to mitigate. The IHIN may facilitate the mitigation process if asked and if practicable for the IHIN to do so.

4. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Privacy Policy 11: *Breach Investigations and Incident Response*

Scope and Applicability: This Policy applies to the IHIN and all Participants.

Policy: The IHIN, all Participants and their BAs and contractors shall investigate, respond to and report privacy Breaches related to the IHIN in compliance with applicable federal and state law.

Standards:

1. **Duty to Investigate.** Each Participant shall promptly investigate reported or suspected privacy Breaches implicating privacy or security safeguards deployed by the IHIN (or its contractors) according to its own policies. Participant shall notify the IHIN of reasonably likely and confirmed Breaches, and shall notify Other Participants if the Participant knows or reasonably believes they have been the subject of unauthorized access, use or disclosure. Participants shall document all Breach investigations and findings and provide a summary of confirmed Breach findings to the IHIN in a manner consistent with HIPAA Breach requirements. The findings shall include the remedial actions, if any, taken for a Breach; remedial actions shall be appropriate to the Breach.

2. **Incident Response.** The IHIN shall implement an incident response system in connection with known or suspected privacy Breaches, whether reported by Participants or discovered by the IHIN. The incident response system shall include the following features, each applicable as determined by the circumstances:

    2.1 Cooperation in any investigation conducted by the Participant or direct investigation by the IHIN;
    2.2 Notification of Other Participants or Authorized Users as need to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the Breach;
    2.3 Cooperation in any mitigation steps initiated by the Participant to the extent possible;
    2.4 Furnishing audit trails and other information helpful in the investigation;
    2.5 Developing and disseminating remediation plans to strengthen safeguards or hold Participants or IHIN's Authorized Personnel accountable;
    2.6 Any other steps mutually agreed to as appropriate under the circumstances; and
    2.7 Any other step required under the security incident reporting and investigation system contained in the Security Policies.

3. **Department Cooperation.** The IHIN shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, if and when the investigation implicates the IHIN's Authorized Personnel's conduct, the conduct of another Participant or Authorized User, or the adequacy or integrity of IHIN safeguards.

4. **Participant Cooperation.** Each Participant shall cooperate with the IHIN in any investigation of the privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the IHIN or the Other Participant, if and when the investigation implicates such Participant's compliance with the IHIN policies or the adequacy or integrity of IHIN safeguards.

5. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.

IHIN Privacy Policy 12: *Authorized Personnel and Authorized User Controls*

Scope and Applicability: This Policy applies to the IHIN and all Participants. This Policy is to be read and applied in conjunction with the IHIN Security Policies.

Policy: The IHIN and all Participants shall be responsible for designating, training, supervising, and ending access to the IHIN by IHIN's Authorized Personnel and Participant's Authorized Users, respectively.

Standards:

1. **Participant Responsibilities.** Each Participant is responsible to:

   1.1 Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these Privacy Policies and to receive notices on behalf of the Participant. For Participants that have their own system administrator, this shall ordinarily be the system administrator.

   1.2 Designate its own Authorized Users from among its Workforce, and designate BAs and contractors (or designate from among their Workforce) authorized to act as Authorized Users on the Participant's behalf.

   1.3 Train and supervise its Authorized Users and require any BA or contractor to train and supervise its Authorized Users consistent with the Participant's privacy policies, these Privacy Policies, the Security Policies and with the terms of the BAA, as applicable.

   1.4 If Participant connects to the IHIN from the Participant electronic health record system, Participant shall, in a timely manner, suspend, limit or revoke access authority upon a change in job responsibilities or employment status of an Authorized User. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.

   1.5 If Participant amends connection method to the IHIN through the clinical portal or a Direct Secure Messaging account, Participant shall, in a timely manner, notify the IHIN of the change so that the IHIN may revoke access authority. Notification shall occur prior to, contemporaneously with, or in a timely manner following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.

   1.6 Hold their Authorized Users accountable for compliance with the IHIN's and the Participant's policies and, as applicable, the terms of any business associate agreement.

2. **Department Responsibilities.** The IHIN is responsible to:

2.1 Grant access to Participants, subject to reserved authority to suspend, limit, or revoke such access authority.

2.2 Train and supervise its Authorized Personnel on these Privacy Policies, the Security Policies and the standard terms required by the BAA.

2.3 Suspend, limit or revoke access authority for its Authorized Personnel in a timely manner in the event of Breach or non-compliance, as required by these Privacy Policies, the Security Policies or the terms of the BAA.

2.4 Immediately limit or revoke access authority upon a change in job responsibilities or employment or contract status of its Authorized Personnel.

2.5 Suspend, limit, or revoke the access authority of a Participant on its own initiative and in a timely manner upon a determination that the Participant has not complied with these Privacy Policies, the IHIN Security Policies or the terms of the Authorized User agreement, if the IHIN determines in its sole discretion that doing so is necessary for the privacy of individuals or the security of the IHIN. The procedures for granting and revoking access authority are contained in the Participation Agreement.

3. **Application to BAs and Contractors.** Participants agree to apply this policy or standards equivalent to those in this policy to their BAs and to the contractors and subcontractors of their BAs that may have access to PHI through the IHIN as the Participant deems appropriate through the terms of their business associate agreements.