190 N. Independence Mall West, Suite 701 Philadelphia, PA 19106 www.healthshareexchange.org

Version	Approval Date	Owner
1.0	TBD	Don Reed

TPO Uses & Disclosures in Alignment with HIPAA

1. Purpose

The purpose of this Use Case is to align permitted uses and disclosure of Data through HSX with federal laws which support and, under certain circumstances, require the sharing and exchange of electronic health information (EHI), including electronic protected health information (EPHI), for treatment, payment and health care operations (**TPO**) in accordance with all other applicable laws.

The HIPAA Privacy Rule establishes a foundation of Federal protection for individuals' protected health information (PHI) while carefully balancing those protections to avoid creating unnecessary barriers to the delivery of quality health care. As such, the HIPAA Privacy Rule generally prohibits a Covered Entity from using or disclosing PHI unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities.[(a)] The Secretary of HHS has said that access to Treatment and efficient Payment for health care, both of which require use and disclosure of PHI, are essential to the effective operation of the health care system. In addition, certain Health Care Operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for Healthcare Providers and Health Plans, are essential to support Treatment and Payment. Most Individuals expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the Covered Entity's health care business. To avoid interfering with an Individual's access to quality health care or the efficient payment for such health care, the HIPAA Privacy Rule permits a Covered Entity to use and disclose PHI, with certain limits and protections, for TPO activities.

On May 1, 2020, the Office of National Coordinator for Health Information Technology (ONC) promulgated a final rule implementing certain provision of the 21st Century Cures Act, which included defining "reasonable and necessary" activities that do not constitute information blocking (aka, the "Information Blocking Rule"). Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of EHI, except as required by law or specified in an information blocking exception. The Cures Act applied the law to healthcare providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs). The implementation of the Information Blocking rule is intended to advance interoperability and support the access, exchange, and use of EHI, which includes electronic PHI (EPHI). Healthcare providers who are determined by OIG to have committed information blocking and for which OIG refers its determination to CMS would be subject to disincentives. HIEs/HINs and health IT developers of certified health IT that are found to violate the Information Blocking Rule would be subject to civil monetary penalties.

Finally, federal agencies are rapidly coordinating efforts and policies to promote interoperability and sharing of EHI across the healthcare ecosystem. By way of example, ONC designated The Sequoia Project as the Recognized Coordinating Entity (RCE) charged with developing, implementing, and maintaining the Common Agreement component of the Trusted Exchange Framework and Common Agreement ("TEFCA℠"). The Common Agreement creates the baseline technical and legal requirements for HIEs/HINs to share EHI and is part of the mandate under the 21st Century Cures Act. The TEFCA supports the sharing of EHI for TPO.

This Use Case is intended to position HSX and its Participants to be able to participate in all legally permitted sharing of Data for TPO purposes in accordance with applicable law and the Participation Agreement, which recognizes TPO as Permitted Purposes for which Data may be shared through HSX.

2. Scope

A. This Use Case shall apply to all Participants of HSX who have successfully completed HSX's "onboarding" process, irrespective of type (e.g., Covered Entity, public health authority, social service agency, Business Associate) unless the Participant is prohibited by law from accessing, using or disclosing EHI/EPHI for the TPO purposes described in this Use Case. *By way of example*, EPHI shall not be disclosed to a Health Plan for payment or health care operations if an Individual has paid for a health care item or service out of pocket, in full, and requested that their EPHI not be share with their Health Plan.

B. For Participants of HSX that are Healthcare Providers and Health Plans but not a Covered Entity or as defined under HIPAA, such Participants shall abide by HIPAA and the HIPAA Privacy Rule as if they were a Covered Entity with regard to how they access, use and disclose EPHI for TPO purposes.

C. For Participants of HSX that are a Business Associate of a Covered Entity, such Business Associate Participant shall abide by HIPAA and the HIPAA Privacy Rule when requesting EPHI on behalf of its contracted Covered Entity customer. A Business Associate may not initiate a request for EPHI solely for its own Healthcare Operations.

D. Participants of HSX that are a Health Plan may **not** use this TPO Use Case to Query or access EPHI for the purpose of analysis of the costs, rates, charges, utilization levels or for steering or tiering HSX Participants that are hospitals, health care systems or other types of health care providers.

E. This Use Case shall apply to all Data eligible for access and transmission through or by HSX unless such Data is prohibited under applicable law(s) from being shared because consent/authorization for TPO and was not obtained and there is no applicable exception to such consent/authorization requirement. To this end, it is noted that the HIPAA Privacy Rule does not require a signed HIPAA Authorization for any Covered Entity or Business Associate on their behalf, to share EPHI for TPO purposes, so long as the other conditions of the HIPAA Privacy Rule are met. Participants that contribute EPHI to or though HSX are responsible for ensuring that all other legally required consents/authorizations are obtained from Individuals to permit their Data to be fully shared for TPO purposes.

The following type of Data and access will NOT be available for this Use Case unless otherwise noted:

- **"Opted Out" individuals**: There shall be absolutely **no access** to, use or disclosure of Data of individuals who have opted out of HSX, except when Data is De-Identified Data.

- **"Out-of-Pocket Payment" Restricted Data**. EPHI associated with an item or service for which an Individual has paid for out of pocket, in full, and requested a restriction on their EPHI being shared with their Health Plan shall not be made available to such Health Plan that may be requesting EPHI for any Payment or Health Care Operation. The foregoing restriction does not apply to Treatment disclosures, which may still occur despite any such requestion restriction.

- **Super Protected Data (SPD)**[1] that the Individual has ***not*** consented to/authorized for Treatment, Payment and Health Care Operations uses and disclosures and for which there is ***no exception*** to consent/authorization under the applicable federal or state law shall **not** be made available to any Participant requesting such SPD for TPO purposes. For purpose of this Use Case, Super Protected Data or SPD means types of EPHI for which federal and/or state laws requires a specific consent or authorization before it may be used or disclosed for Treatment, Payment or Health Care Operations. Each data-contributing Participant remains solely responsible for "filtering out" (i.e., not sending) SPD to prevent it from being shared with or through HSX *unless* proper consent has been obtained or HSX has expressly taken on responsibility for filtering such data on Participant's behalf (e.g., HIV/AIDS information).

F. **Hierarchy and Interpretation.** This Use Case does not "override" requirements or restrictions contained in any other HSX-approved Use Case which governs a specific type of use and disclosure of EHI. That is, generally, if a different HSX-approved Use Case governs a specific type of TPO use and disclosure, the Participant must follow the procedures and any restrictions contained in the more specific Use Case when requesting, using and disclosing EPHI for such TPO purpose; and this TPO Use Case does not authorize a Participant to disregard those specific requirements and restrictions. By way of example, a Participant that wishes to request EPHI for population health purposes, a type of Health Care Operation, must follow the HSX-approved Use Case "*Participants Population Health Use Case".* Additionally, EPHI that is desired for "research" purposes may not be requested under this TPO Use Case and must follow an HSX-approved Use Case governing research (i.e., *Patient-Authorized Research* Use Case). Any Participant that is unsure if its Query for EPHI would be considered a "Health Care Operation" or "Research" purpose shall NOT initiate any such Query before confirming the intended Query purpose with HSX's Privacy Officer.

[1] Note: For purposes of this policy, Super Protected Data (SPD) is defined purposefully to not include PHI that potentially relates to reproductive health care (hereinafter, RHC-PHI"). While uses and disclosures of RHC-PHI are regulated and restricted by HHS' final rule "*HIPAA Privacy Rule to Support Reproductive Health Care Information"* (89 Fed Reg 32976 (April 26, 2024)), those requirements do **not** apply to treatment, payment or health care operations purposes. For further information regarding specific requirements and restrictions on RHC-PHI, see HSX's Policy "*Reproductive Health Care Privacy*".

3. Policy

Subject to all other HSX-approved Use Cases governing a specific type of TPO purpose (e.g., Population Health), HSX permits all Participants to request Data, including EHI and EPHI, for any Treatment, Payment, and Health Care Operation purpose.

HSX responds to all such requests by making the requested Data available for TPO purposes unless it is otherwise restricted from access, use and disclosure as set forth under the Scope section above.

4. Procedure

A. Participants that are Covered Entities and contribute Data to HSX shall ensure that all Individuals who are patients (Healthcare Provider) or members/beneficiaries (Health Plan) have received a copy of their HIPAA Notice of Privacy Practices setting forth how Individuals' EPHI may be accessed, used and disclosed for TPO purposes. Such Participants shall also ensure that the consent/authorizations collected from Individuals authorize the use and disclosure of EPHI for TPO purposes.

B. Data will be disclosed to the requesting Participant for the Treatment activities of any Healthcare Provider (including providers that are not covered by the HIPAA Privacy Rule).

C. Data will be disclosed to any other Covered Entity or a Healthcare Provider (including providers not covered by the HIPAA Privacy Rule) for the Payment activities of the entity that receives the information.

D. Data will be disclosed for certain Health Care Operation activities of the entity that receives the information **but only if**:

- Each entity either **has or had a treatment relationship** (Healthcare Provider) or **insured/beneficiary relationship (Health Plan)**, as the case may be, with the Individual who is the subject of the information, and the EPHI pertains to the relationship; **and**

- The disclosure is for a **quality-related Health Care Operations activity** (i.e., the activities listed in paragraphs (1) and (2) of the definition of "Health Care Operations" at 45 CFR 164.501), for subscriber/member **underwriting** (i.e., an activity listed in paragraph (3) of the definition of "Health Care Operations" at 45 CFR 164.501), for conducting or arranging for a **medical review** (i.e., an activity listed in paragraph (4) of the definition of "Health Care Operations" at 45 CFR 164.501), or for the purpose of **health care fraud and abuse** detection or compliance. For example: A health care provider may disclose EHPI to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the Individual who is the subject of the information.

E. To the extent permitted in this Use Case and subject to the limitations contained herein, Data will also be disclosed:

- If such disclosure is required to comply with applicable law including, but not limited to, the Information Blocking Rule and TEFCA;

- As required by any QHIN in which HSX participates; and/or

- In accordance with the requirements of any External Networks in which HSX participates including, but not limited to, the eHealthExchange, P3N, NJ HIN, CRISP, DHIN and PCC.

F. **Minimum Necessary.** A requesting Participant must have policies and procedures implemented that reasonably limit Participant's uses and disclosures of, and requests for, EPHI for Payment and/or Health Care Operations to the minimum necessary in accordance with the HIPAA Privacy Rule. A requesting Participant also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to EPHI for Payment and Health Care Operations, based on those who need access to the information to do their jobs. Participants are not required to apply the minimum necessary standard to uses, disclosures to or requests by a Healthcare Provider for treatment purposes. By submiting a Query for Payment or Health Care Operations the requesting Participant is representing to HSX and other Participants that it is requesting only the minimum necessary EPHI needed for such purpose. Such representation shall be imputed to the requesting Participant when a Query for Payment or Health Care Operations is submitted by an authorized workforce member of Participant. Participant acknowledges and agrees that HSX generally relies on such representation when returning responsive EPHI for such purposes. Notwithstanding the foregoing, HSX reserves the right to review, reject or narrow the scope of a response to a Participant's Query to ensure compliance with HIPAA's minimum necessary standards.

G. **When technologically feasible, HSX may facilitate segmenting and filtering SPD so that it is not shared for TPO because preconditions of consent have not been met and there is no applicable exception to consent. Coordination of any consent management and/or data segmentation/filtering between HSX and Data-contributing Participants shall be agreed upon in advance.**

5. Enforcement

HSX's Chief Security Officer and Chief Privacy Officer are responsible for enforcing compliance with this Use Case under the direction of the HSX President.

In the event a misuse of Data is alleged or identified, including any failure by Participant to meet a requirement under this Use Case that is a condition of submitting a Query (e.g., Minimum Necessary obligations under Paragraph 4.F.), HSX shall follow the procedure outlined in the HSX Data Misuse Policy. HSX monitors the use of all Data, including PHI under this Use Case, in accordance with the Audit and Monitoring Policy.

6. Definitions.

For purposes of this TPO Use Case, and notwithstanding anything to the contrary in the Participation Agreement and the *Glossary*, the following terms shall have the following definitions:

"HIPAA Privacy Rule" shall mean the regulations set forth at 45 CFR Parts 160 and 164, Subparts A and E.

"Health Care Operation" has the meaning assigned to such term at 45 C.F.R. § 164.501, as may be amended from time to time. For ease of reference, "health care operations" is defined in the HIPAA Privacy Rule to mean any of the following activities of a covered entity to the extent that the activities are related to covered functions: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Except as prohibited under § 164.502 (a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514 (g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (iii) Resolution of internal grievances; (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of § 164.514 , creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

"Payment" has the meaning assigned to such term at 45 C.F.R. § 164.501, as may be amended from time to time. For ease of reference, "payment" is defined in the HIPAA Privacy Rule to mean: (1) The activities

undertaken by: (i) Except as prohibited under § 164.502 (a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) Name and address; (B) Date of birth; (C) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the health care provider and/or health plan.

"Treatment" has the meaning assigned to such term at 45 C.F.R. § 164.501, as may be amended from time to time. For ease of reference, "treatment" is defined in the HIPAA Privacy Rule to mean: the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

For a complete list of definitions, refer to the *Glossary*.

7. References

(a) HHS Guidance Materials, "*Uses and Disclosures for Treatment, Payment, and Health Care Operations*." www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html.

Policy Owner	Privacy Officer	Contact	Don.reed@healthshareexchange.org
Approved By		Approval Date	
Date in Effect		Version #	1**Error! No document variable supplied.**
Original Issue Date		Last Review Date	

Related Documents	Data Misuse Policy Audit and Monitoring Policy Glossary