SAN DIEGO HEALTH CONNECT

PARTICIPANT POLICIES AND PROCEDURES

[Version Date: December 2023]

I. HEALTH INFORMATION EXCHANGE OVERVIEW:

Exchange Goals: The San Diego Regional Health Information Exchange ("SDHC") is designed to facilitate the quick, safe, and secure access to and exchange of health information among health care organizations situated throughout San Diego and Imperial County. By making this information available through a health information exchange (the "Exchange" or "HIE"), health care organizations can quickly view the information together in one place when healthcare decisions are being made. SDHC also permits access to the Exchange by government agencies to carry out public health activities, such as gathering immunization records and monitoring and reporting outbreaks of communicable diseases and other public health concerns in a timely manner.

Building Trust: In order to build and maintain trust within the Exchange Community, protect patient healthcare information, and promote the efficiency and security of the Exchange, SDHC's goal is to ensure the highest levels of privacy and security practices by SDHC and each individual or entity participating in the Exchange.

Prior to such participation, SDHC shall confirm that each individual or entity requesting to participate in the Exchange qualifies as an eligible individual or entity to participate. Eligible individuals or entities may include a health care provider (such as physicians, medical groups, independent physician association), hospitals, clinics, laboratories, emergency medical services (EMS) agencies, pharmacies, government agencies, health plans, insurers, or other payors, as well as business associates of any of the above, in addition to certain social service or community-based organizations. Only individuals or entities that enter into a Participation Agreement with SDHC shall be permitted to access the Hosted System and use the Services (each a, "Participant", and collectively "Participants").

As part of SDHC's goal to ensure the highest levels of privacy and security practices by it and Participants, SDHC has developed the following Policies and Procedures. These are intended to set forth uniform standards that apply to each Participant and to work hand-in-hand with each Participant's internal security and privacy policies and procedures, as a matter of complying with Applicable Law, including but not limited to HIPAA, the HITECH Act, and CMIA.

These Policies and Procedures are incorporated by reference into the Participation Agreement that each Participant is required to execute before accessing the Exchange and using the Services provided by SDHC, and may be amended, repealed and/or restated in accordance with the Participation Agreement. The failure of a Participant to comply with any of the Policies and Procedures outlined below may result in the termination of the Participant's right to access the Exchange.

Exchange Board of Directors and Advisory Work Groups: SDHC is a non-profit public benefit corporation. Its Board of Directors is composed of local volunteer community representatives. Participating organizations are encouraged to take an active role in the Exchange through involvement with an Exchange work group ("Work Groups"). Such participation allows the Participant to have direct input into the formulation of and updates to these Policies and Procedures. SDHC also has established a number of Work Groups that provide input and guidance to the Board of Directors on such matters as Subscription Fees for accessing the Exchange, Patient consent requirements (e.g., opt-in or opt-out), and privacy and security policies.

Definitions: Terms used but not otherwise defined in these Policies and Procedures, inclusive of the Glossary Section, shall have the same meaning given to them in the Participation Agreement or the Business Associate Agreement.

II. PATIENT DATA

POLICY: SDHC's Hosted System is programmed to search for, retrieve and deliver discrete types of Patient Data. It is SDHC's policy to require Participants comply with all Applicable Law and the Participation Agreement in sharing Patient Data, and to ensure that Patient Data be stored electronically in commonly accepted electronic formats that are compatible with most up-to-date integration standards.

PROCEDURE:

The Hosted System will display Patient Data from an electronic record maintained by a Participant. As permitted by Applicable Law, the Patient Data may include, but is not limited to, the following information with regard to each individual patient or member whose Patient Data is contributed to the Hosted System by a Participant (the "Patient"): Allergies, Goals, Problems, Assessment Plans, Health Concerns, Procedures, Care Team Members(s), Immunizations, Clinical Notes, Laboratory, Smoking Status, Medications, Clinical Tests, Patient Demographics/Information, Vital Signs, Diagnostic Imaging, Encounter Information.

Participants shall maintain a continuous (except for Downtime) connection to the Hosted System in order to allow the Participant's Patient's electronic records (i.e., Patient Data) to be retrieved or sent to and from the Participant's internal electronic database to the Exchange Community. The Patient Data will be sent by a Participant to the Exchange via standard-based formats as scoped by SDHC.

Any information that is classified as Sensitive Health Information (as defined below) will be identified by the Participant and handled in accordance with SDHC's Sensitive Health Information Policy and Procedure.

III. SENSITIVE HEALTH INFORMATION

POLICY: Certain Protected Health Information may require additional measures before Applicable Law permits such Patient Data to be shared and accessed through the Exchange, including but not limited to: (i) Psychotherapy Notes; (ii) Patient Data subject to Part 2; (iii) information from state-sponsored substance abuse treatment programs protected by California Health and Safety Code § 11845.5; (iv) certain outpatient psychotherapy records in accordance with the CMIA; (v) records of persons receiving mental health services protected by the Lanterman-Petris-Short Act; (vi) records of persons receiving services for developmental disabilities protected by the Lanterman Developmental Disabilities Services Act; and (vii) HIV test results(collectively, "Sensitive Health Information"). Sensitive Health Information also includes any Patient Data of a Patient who has exercised their right under HIPAA (45 C.F.R. § 164.522(a)(1)(vi)(B)) to prohibit disclosures to a health plan or payor of information relating to healthcare items or services for which the Patient has paid in full out-of-pocket.

PROCEDURE:

SDHC currently does not receive or exchange any SHI except as permitted by Applicable Law (e.g. with Patient's Authorization).

IV. PATIENT CONSENT

POLICY: The Exchange generally operates as an opt-out health information exchange, meaning that Patients who do not choose to share their data with other Participants in the Exchange Community must explicitly opt-out of participation.

PROCEDURE:

Participants are responsible for notifying their Patients of the opportunity and the benefits of sharing their Protected Health Information with other Participants of the Exchange Community through the HIE, including information in their Notice of Privacy Practices regarding the Exchange and a description of how Patients may execute an opt-out.

Patient Data of a Participant's Patient will be made available to other Participants for a Permitted Use (as defined below) through the Exchange unless and until the Patient affirmatively opts-out and the Participant has notified SDHC of the Patient's decision to opt-out. Upon receipt of a Patient's opt-out status from a Participant, SDHC will promptly ensure that the Patient's opt-out status is effective and reflected in the Hosted System.

When a Patient opts-out, the Exchange may still receive Patient Data regarding the Patient from a Participant; however, SDHC will implement security and access controls to prevent other Participants from accessing that Patient's Patient Data, except as permitted by Applicable Law, such as pursuant to a Patient's Authorization or in the event of a qualifying medical emergency via "break the glass", following which the Participant shall provide an attestation to SDHC documenting the basis for accessing such Patient Data. For example, in the case of Patient Data subject to Part 2, the attestation shall detail how the disclosure was necessary to meet a bona fide medical emergency in compliance with Part 2.

Patients may also contact SDHC for information about how to exercise their right to opt-out.

The Exchange only receives opted-in data from Community Information Exchange (CIE).

III. PERMITTED USES

POLICY: Participants (and their Authorized Users) must comply with all Applicable Law related to the use and disclosure of Patient Data through the Exchange, as well as with the Participation Agreement and Policies and Procedures, and have a duty to safeguard Protected Health Information obtained through the Exchange appropriately and to comply with the restrictions set forth in these Policies and Procedures, and in the Participation Agreement.

In accordance with Applicable Law, Participants (and their Authorized Users) may only access, use, and disclose Electronic Protected Health Information (or "ePHI") for a Permitted Use, as defined below.

Any access of Patient Data is subject to audit at SDHC's sole discretion to ensure that access by a Participant was in accordance with these Policies and Procedures, and Applicable Law.

PROCEDURE:

1. Permitted Access to and Use of Patient Data:

The level of access a Participant has to Patient Data is role-based and will depend on the Participant's eligibility status, as determined by SDHC. For example, the level of access is denoted "Unlimited" for health care providers (as defined by HIPAA) (such as hospitals, clinics, medical groups, and physicians), "Limited" for government agencies, community-based organizations, and health plans/payors, and "View Only" for system-testing and other limited purposes by SDHC's Business Associates. This level of access is monitored by the Exchange Administrator. Each Participant is responsible for training, supervising and monitoring its Authorized Users' access and use of the Hosted System and ePHI to ensure that data is being accessed for Permitted Uses only.

The permitted uses of Patient Data obtained through the Exchange are only for the following purposes, as permitted by Applicable Law (collectively, "Permitted Uses"):

a. Healthcare Providers may only view, access, use, or disclose Patient Data pertaining to their Patients for (i) Treatment; (ii) Payment; (iii) Health Care Operations; (iv) public health activities as set forth under HIPAA at 45 C.F.R. §§ 164.512(b) or 164.514(e); (v) uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or a person who has the authority to consent to the disclosure of a Patient's Patient Data under Applicable Law ("Personal Representative"); or (vi) for such other purpose permitted by Applicable Law.

b. Health plan/payor Participants may only view, access, use, or disclose Patient Data of current members or enrollees of the Participant, and will not view any Patient Data of individuals who are not current members or enrollees of that Participant, for: (i) Payment; (ii) Health Care Operations; (iii) public health activities as set forth under HIPAA at 45 C.F.R. §§ 164.512(b) or 164.514(e); (iv) uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or their Personal Representative; or (v) for such other purpose permitted by Applicable Law.

c. Government Participants (that are not otherwise a Healthcare Provider) may only view, access, use, or disclose Patient Data for: (i) public health activities as set forth under HIPAA at 45 C.F.R. §§ 164.512(b) or 164.514(e); (ii) uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or their Personal Representative; (iii) uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or their Personal Representative; or (iv) for such other purpose permitted by Applicable Law.

d. Social Service/Community-Based Organizations (that are not otherwise a Healthcare Provider) may only view, access, use, or disclose Patient Data for: (i) Treatment; (ii) uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or their Personal Representative; or (iii) for such other purpose permitted by Applicable Law.

d. Notwithstanding the foregoing, in the case of Sensitive Health Information, Participants will comply with SDHC's Sensitive Health Information Policy and Procedure, the Participation Agreement, and all Applicable Laws regarding any use of such information.

2. Prohibited Uses of ePHI: Participants (and their Authorized Users) must not use or permit the use of the Exchange or Patient Data for any prohibited use, which shall include: (i) Sharing ePHI with a third person or entity that is not affiliated with the Participant or SDHC, (ii) providing separate services or sub-licenses to a third party, (iii) sharing an Authorized User's log-on user name or password with a person that is not an Authorized User Administrator or SDHC's Administrator, (iv) aggregating ePHI to compare the performance of other Participants and/or Authorized Users, (v) Marketing and/or fundraising purposes, (vi) any sale of ePHI prohibited by Applicable Law, (vii) in order to unlawfully discriminate or unlawfully deny or limit access to medical services, or prosecute or take any other adverse action against an individual who accesses medical services, or (viii) in any manner that is otherwise prohibited by Applicable Law.

3. Internal Policies: Each Participant must adopt, implement, and enforce internal policies and procedures that comply with Applicable Law, including but not limited to HIPAA, the HITECH Act, and implementing regulations, to ensure that Patient Data accessed or used from the Hosted System is being accessed or used only for a Permitted Use. Each Participant must train and monitor their Authorized Users' use of Patient Data and the Hosted System to ensure compliance with the Participation Agreement, these Policies and Procedures, and all Applicable Law.

4. Minimum Necessary: With the exception of Treatment purposes and uses and disclosures pursuant to an Authorization provided by the Patient who is the subject of the Patient Data or their Personal Representative, each Participant will make reasonable efforts to limit information accessed or used through the Hosted System to the minimum amount necessary to accomplish the intended Permitted Use purpose for which it is being accessed or used. Additionally, during the process of querying the Hosted System for Patient Data for a Permitted Use, Participants will (i) implement safeguards to minimize unauthorized incidental disclosures of Patient Data, (ii) include the minimum amount of demographic information reasonably necessary to enable Authorized Users to successfully identify a Patient, and (iii) prohibit, or restrict to the extent reasonably possible, Authorized Users from accessing Patient Data in any manner inconsistent with these Policies and Procedures.

IV. QUALITY AND ACCURACY OF THE MASTER PATIENT INDEX - "MPI"

POLICY: Every Participant is responsible for regularly maintaining and correcting its internal electronic medical records database, including the types of information used to compile the Exchange's Master Patient Index or "MPI". Because the Hosted System is based on positive matches identified through the MPI, it is incumbent upon all Participants to enter complete and accurate information for all Patient identifiers specified herein in their medical records database.

PROCEDURE:

1. **Maintaining an accurate MPI.** When a Participant is notified by SDHC or when it discovers that information in a Patient's medical record is duplicated or incomplete, the Participant should follow the Participant's established processes to investigate and determine if their database contains duplicate or incomplete records. If the record is updated or corrected, then the Participant should notify SDHC within one (1) business day when the update has been completed so that SDHC can link or unlink the Patient's files as instructed by the Participant.

2. **Adding a New Patient Record:** At a minimum, to add a Patient to the Exchange's MPI, the Participant's data feed must include the following information: the Patient's medical record number, the Patient's first and last name, the Patient's date of birth, the Patient's gender, and if available, the Patient's middle initial and SSN.

V. AUTHORIZED ACCESS TO THE HOSTED SYSTEM

POLICY: Only Authorized Users are permitted access to ePHI through the Hosted System. To limit access to Authorized Users, SDHC has implemented certain methods designed to help Participants ensure that only their Authorized Users access the Hosted System. SDHC will work with the appropriate management to define user roles.

PROCEDURE: SDHC offers various methods for Participants and their Authorized Users to view Patient Data on the Hosted System. In consultation with the Participant, SDHC will determine the best method for the Participant as part of the "on-boarding" process. The method selected will correspond to the Participant's role-based level of access to the Hosted System and the specifications of the Participant's own internal computer system and electronic medical records database. Regardless of the method implemented, Participants must monitor access to the Hosted System by their Authorized Users to ensure compliance with Applicable Law, including but not limited to safeguarding the privacy and security of Patient Data, whenever accessing the Hosted System. As part of this process, SDHC has the following procedures regarding each Participant's obligation to establish a User Administrator and identify Authorized Users:

1. Establish a "User Administrator": Each Participant must designate at least one "User Administrator" to serve as the point of contact between the Participant and Exchange. The User Administrator will be the individual responsible for gathering, screening and submitting requests to SDHC for Authorized User identification keys and for notifying SDHC of changes in Authorized Users' permissions and of the termination of Authorized Users employment. The User Administrator will also be responsible for communicating with SDHC regarding requests for replacement passwords and the deletion or modifications of user identification keys.

2. Qualified Authorized Users: The User Administrator will screen the individuals who will be designated by the Participant as Authorized Users to be sure they meet the requirements of the Participation Agreement's certification criteria for Authorized Users, including but not limited to receiving appropriate privacy and security training, as required by the Participation Agreement and Applicable Law.

3. Registration of Authorized Users: SDHC will only allow those individuals who have been designated an Authorized User by the Participant's User Administrator to register with and obtain log-on credentials to access the Hosted System. SDHC Support will provide the User Administrator with specific training on the methods to complete the registration of an Authorized User and train them on how to use the Hosted System. Once this is done, SDHC will send the newly registered Authorized User an email with the user identification key and generic password to log on to the Hosted System. The Authorized User will then be instructed to change the password upon initial login to the Exchange. If an Authorized User experiences any problems with or questions about the account in the future, such as lockout accounts or insufficient privileges to access data, Authorized Users should contact their User Administrator to contact SDHC Support. The User Administrator(s) shall maintain a record of all Authorized Users and shall provide a list in a medium and format requested by SDHC identifying all of Participant's Authorized Users. SDHC shall have the right to audit the accuracy and completeness of that list at any time and for any reason, and the User Administrator shall assist SDHC in carrying out such audit.

4. *Deactivation of Authorized User Account.* Participant shall sanction Authorized Users who fail to act in accordance with the Participation Agreement, the Policies, or in accordance with the Participant's disciplinary policies and procedures and Participant shall notify SDHC as promptly as reasonably possible but in any event within one (1) calendar day after Participant becomes aware that an Authorized User has violated or threatened to violate the Participation Agreement and/or Policies and Procedures so that SDHC may, in its discretion, temporarily or permanently deactivate the Authorized User's account. Further, whenever an Authorized User's employment has been terminated or an Authorized User's rights have been changed by the Participant and/or User Administrator, the User Administrator must immediately notify SDHC. If an Authorized User's account has had no activity for a period of ninety (90) calendar days, SDHC may deactivate the Authorized User's account.

5. *Termination of Participation Agreement.* Upon termination of its Participation Agreement with SDHC for any reason, that Participant, its User Administrator and its Authorized Users will cease to have any rights to access and use the Hosted System or Services. SDHC shall ensure that access to the Hosted System and/or the Services shall be immediately terminated.

VI. SECURITY OF THE HOSTED SYSTEM

POLICY: Each Participant will have in place appropriate security policies and implement reasonable administrative, physical, and technical safeguards to ensure their security requirements meet or exceed industry best practices. Each Participant is responsible for the security of ePHI while interacting with the

Hosted System. Participants must ensure that their own internal computer systems are protected from a Breach of Privacy or Security or the unlawful disclosure of ePHI while an Authorized User is interacting with the Hosted System. Each Participant is required to assess the risks and vulnerabilities of their internal computerized medical record database and adopt and implement policies and procedures that address those risks.

PROCEDURE:

1. Participant Security Obligations.

a. **Each Participant must monitor and audit all access to and use of the Hosted System.** The Participant is responsible for monitoring access to the Hosted System, and will be responsible for maintaining a secure environment that supports the operation and continued development of the performance and service specifications, and to ensure that Patient Data is readily available to the Exchange Community through a secure connection between their internal patient records database and the Hosted System.

b. Participants shall use appropriate safeguards to prevent use or disclosure of Patient Data other than as permitted by these Policies and Procedures, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of Patient Data as required by Applicable Law.

c. Each Participant will, as appropriate under HIPAA and/or other Applicable Law, have written privacy and security policies in place and will enforce such policies with regard to access to the Hosted System. Participants will regularly review their privacy and security policies to ensure compliance with Applicable Law.

d. Participants will comply with all Applicable Law and industry practices regarding system security, including meeting the standards established by HIPAA pertaining to system and workstation security, and will also be required to comply with any performance and service specifications or operating protocols or procedures adopted by SDHC that define expectations for Participants with respect to enterprise security.

e. Each Participant shall be responsible for procuring, and assuring that its Authorized Users have, or have access to, all equipment and software necessary to access the Hosted System. Each Participant shall ensure that all computers and electronic devices owned or leased by the Participant and its Authorized Users to be used to access the Hosted System are properly configured.

VII. HOSTED SYSTEM SUPPORT

POLICY: Each Participant is responsible for maintaining internet and internal network connectivity and providing such other system support services as may be necessary to: (i) transmit Participant's Patient data to the Hosted System; (ii) provide online access to the Hosted System; (iii) cooperate with SDHC in maximizing the performance and availability of the Hosted System for Participants and Authorized Users.

PROCEDURE:

Each Participant is responsible for: (i) maintaining internet and internal network connectivity and for the performance of the Hosted System as limited by that connectivity; (ii) adding SDHC domain names to access control or other security systems to permit access from Participant's network; (iii) providing the first level of support to its Authorized Users relating to access to and performance of the Hosted System that can then be escalated, if necessary, to SDHC Support; (iv) cooperating with SDHC Support personnel in troubleshooting any incidents experienced by Authorized Users with respect to access to and performance of the Hosted System; (v) designating User Administrators and security administrators who will provide access to appropriate Authorized Users as set forth in these Policies and Procedures; (vi) and cooperating as reasonably necessary and at reasonable times with SDHC and its vendors in testing and implementing upgrades to the Hosted System.

Participants will also monitor data feeds from its computer systems to the Hosted System and address any problems that may arise with respect to such data feeds, ensuring accurate and complete loading of clinical data from its computer systems to the Hosted System. When a Participant detects a problem transaction, it will inform SDHC's technical team in a timely manner of any Patient Data structure or format problems. If there is a change to the format of any Patient Data coming into the Exchange, the Participant's interface engineers must notify SDHC's technical team at least seventy-two (72) hours before the change is made and work with SDHC's technical team on modifying the interfaces appropriately.

VII. LAWFUL DISCLOSURE – MONITORING THE PROPER USE OF ePHI AND INVESTIGATING POSSIBLE BREACH

POLICY: Participants must monitor their Authorized Users' use of ePHI on systems directly associated with Exchange to ensure that ePHI is being used for a Permitted Use and guard against unlawful disclosure of ePHI while an Authorized User is interacting with the Exchange. Each Authorized User should only access the minimum necessary information required for the Permitted Use related to Patients of record. In order to ensure adherence to privacy guidelines and maintain a level of community trust, SDHC will provide audit services to analyze both Participants' use, as well as access to specific Patients, as needed.

PROCEDURE:

1. **Participant Audit Requests:** SDHC will respond to a written request from a Participant for an audit within five (5) working days of receipt of the request. A proper request for such an audit must be in writing and sent to Exchange's Executive Director and the Security and Privacy Officer.

2. Breach Investigation at Participant's Request: A Participant's privacy officer may initiate a suspected Breach of Privacy or Security investigation in the following manner:

a. The privacy officer must send SDHC's Executive Director and Privacy Officer a written request detailing the specifics of the suspected Breach of Privacy or Security.

b. SDHC's Executive Director will notify SDHC's Security Officer, who will investigate the complaint and compile written findings that will be provided to the Participant's privacy officer. As part of the investigation, SDHC's Security Officer will conduct a risk assessment analyzing the probability that the Protected Health Information was compromised, in accordance with Applicable Law.

c. If it is determined that any improper behavior occurred, corrective action will be taken, including, but not limited to revoking an Authorized User's access to the Exchange and issuing a Breach Notification.

3. Breach Investigation at Patient's Request: If a Patient would like to request a formal investigation into suspected inappropriate access to their records, these steps should be followed:

a. The Patient should be instructed to write a letter to Exchange's Security and Privacy Officer giving general (non-health related) information about the incident.

b. SDHC's Security Officer will investigate the complaint, conduct a risk assessment (per above), and compile written findings of the same.

c. If it is determined that any improper behavior occurred, corrective action will be taken, including, but not limited to, revoking an Authorized User's access to the Exchange and issuing a Breach Notification.

VIII. BREACH NOTIFICATION

POLICY: Participants shall maintain internal policies and procedures for quickly and effectively detecting and responding to a Breach of Privacy or Security of its Patients' ePHI and shall comply with the requirements of the Participation Agreement with regard to handling any suspected or confirmed Breach of Privacy and Security and/or Security Incidents.

PROCEDURE:

In the event a suspected or confirmed Breach of Privacy or Security of a Participant's electronic medical record database occurs while a Participant (or any of its Authorized Users) is logged onto the Hosted System, the Participant must immediately commence an investigation of the suspected or confirmed Breach of Privacy or Security and notify both SDHC and all affected Participants as soon as possible, in accordance with the Participation Agreement and Applicable Laws.

Participants must take immediate steps to contain and mitigate any Breach of Privacy or Security and prevent such Breach of Privacy or Security from infecting or affecting the Hosted System. The Participant should immediately disconnect its computer system from the Hosted System until such time as the Breach of Privacy or Security has been identified and corrected, and measures have been implemented to prevent its re-occurrence.

IX. GLOSSARY

"Breach Notification" means a report concerning a Breach of Privacy and Security to a Participant, SDHC, and/or affected Third-Party Participants as set forth in the Participation Agreement and/or Business Associate Agreement/QSOA, in addition to potentially affected individuals and/or government officials, if required by Applicable Law.

"Downtime" means the hosted system is offline and unavailable either due to scheduled or unscheduled maintenance.

"Exchange Administrator" means designated SDHC staff that administers the hosted system.

"Health Care Operations" means those Health Care Operations as defined in 45 C.F.R. § 164.501, including: (i) 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; 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; and (ii) 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. A Participant may only access, view, use, or disclose Patient Data of or from another Participant for Health Care Operations if each either has or had a relationship with the Patient who is the subject of the Patient Data being requested and the Patient Data pertains to such relationship.

“Healthcare Provider” means a Participant that meets the definition of provider under HIPAA and/or the CMIA.

“Payment” means the activities undertaken by (i) a health plan/payor to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a Healthcare Provider or health plan/payor to obtain or provide reimbursement for the provision of health care services. Examples of payment are set forth in the HIPAA regulations at 45 C.F.R. § 164.501.

“SDHC Support” means technical support resources to aid users and troubleshoot system issues.

“Treatment” means the provision, coordination or management of Healthcare and related services among Healthcare Providers or by a single Healthcare Provider, and may include providers sharing information with a third party. Consultation between Healthcare Providers regarding a patient and the referral of a patient from one Healthcare Provider to another also are included within the definition of Treatment. As used herein, uses and disclosures for Treatment purposes includes only those purposes permitted under 45 C.F.R. § 501 and Cal. Civ. Code § 56, et seq.