 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 1 of 17 HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

**1.0 PURPOSE**

To establish policies and procedure related to the operation of and participation in the St. Joseph Health Health Information Exchange (“SJH HIE”).

**2.0 SCOPE**

This policy and procedure shall apply to members of the SJHS workforce, as well as all Participants and Authorized Users.

**3.0 POLICY**


It is the policy of St. Joseph Health System (“SJHS”), as well as persons or entities that contract with SJHS, including Participants (as defined below), when applicable, to comply with federal laws and regulations associated with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, enacted as part of the American Recovery and Reinvestment Act (“ARRA”) of 2009, for access to Protected Health Information (“PHI”), as well as other state and federal laws related to the access to and exchange of Health Information. In the operation of and participation in the St. Joseph Health Health Information Exchange (“SJH HIE”), including a Participant’s access to the Clinical Portal operated by SJHS, SJHS and the Participants must comply with this Policy.

**4.0 PROCEDURES**

**4.1 Compliance with HIPAA; Permissible Use of the SJH HIE**

Participants shall fully comply with the HIPAA Privacy Rule, the HIPAA Security Rule and the HIPAA Breach Notification Rule, when exchanging and accessing Health Information through the SJH HIE. Participants shall be responsible for ensuring that they maintain all appropriate policies, procedures and measures necessary to comply with such requirements, including without limitation, Privacy Rule and Security Rule training, appropriate technical controls when accessing the SJH HIE, audit control processes, and other measures to detect Breaches and Security Incidents involving the SJH HIE.

Participants and Authorized Users are only permitted to use the Clinical Portal to access PHI only for Patients with whom the accessing Participant or its Authorized Users have a Treatment relationship. If a Participant or Authorized User is not documented as having a Treatment relationship with

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 2 of 17 HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

a Patient within the Clinical Portal, then in order to access such Patient’s Health Information through the Clinical Portal, the Authorized User will be required to “Break the Glass” in order to view the Patient’s Health Information through the Clinical Portal. In Breaking the Glass, the Authorized User must indicate the authority that he or she has for accessing the Patient’s Health Information.

Health Information may be exchanged or accessed through the Clinical Portal and using Bi-Directional Exchange for Treatment, Payment, and Health Care Operations activities, as permitted by applicable law, provided that due to legal, technical, and administrative constraints any Health Information disclosed by the SJH HIE to a Participant using Bi-Directional Exchange shall not include HIV test results, mental/behavioral health records, and genetic/hereditary test results. Additionally, depending on the role-based access provisioned to an Authorized User, due to legal and technical constraints, an Authorized User may not have access to all Health Information that is available for exchange through the SJH HIE. For example, an Authorized User with administrative access credentials, will be unable to access a Patient’s full Health Information due to the HIPAA minimum necessary requirements, state limitations and technical constraints.


Health Information will only be permitted to be exchanged as part of Bi-Directional Exchange, subject to the Patient’s right to opt-out or opt-in, as the case may be, if the Patient who is the subject of the Health Information is matched between the SJH HIE and the Participant using the enterprise master patient index to cross-match the Patient.

This Policy does not change or limit any Participant’s access to, or use or disclosure of, PHI entered into the Participant’s EHR System by such Participant’s Authorized Users relating to a Patient encounter at such Participant’s office or facility.

**4.2 Notice of Privacy Practices**

Participants are encouraged to utilize the following specific language in their Notice of Privacy Practices to inform Patients about Participants’ participation in the SJH HIE:

*We may participate in one or more health information exchanges (HIEs) and may electronically share your medical information for treatment, payment and healthcare operations purposes with other participants in the HIEs. HIEs allow your health care providers to*

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>3 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

*efficiently access and use medical information necessary for your treatment and other lawful purposes. [For Participant’s in California: The inclusion of your medical information in an HIE is voluntary and subject to your right to opt-out if you receive services in the State of California. If you do not opt- out of this exchange of information, we may provide your medical information in accordance with applicable law to the HIEs in which we participate. More information on any HIE in which we participate and how you can exercise your right to opt-out can be obtained by contacting us at \_\_\_\_.] [For Participant’s in Texas and New Mexico: If you receive services in the States of Texas or New Mexico, we will not include your medical information in an HIE unless you specifically consent to us doing so. If you opt-out, or do not consent to participating in the HIEs if you receive services in the States of Texas or New Mexico, we will continue to use your medical information in accordance with this notice and applicable law but will not make it available to others through the HIE.]*

If a Participant chooses not to utilize the Notice of Privacy Practices language recommended above, then at the very least the Participant must include in its Notice of Privacy Practices that Participant participates in a health information exchange pursuant to which the Participant may share the Patient’s health information electronically with other providers or entities involved in the provision of care or payment of care for Treatment, Payment, and Health Care Operations purposes. Such Participants must then also ensure that they have adequately informed a Patient of his or her right to opt-out of the SJH HIE or obtained the Patient’s opt-in consent, when required to do so by law.

All Participants shall ensure that Patients receive the patient education materials related to the SJH HIE that have been provided to the Participant by SJHS.

**4.3 Clinical Portal Authorized Users**

Identification of Authorized Users: Participants may request access to the Clinical Portal for any employee or agent that meets the definition of an Authorized User. To request a Unique User Identification and password for an Authorized User, Participants will complete an Authorized User access request form and submit it to [ShareVueHIEProvisioning@stjoe.org](mailto:ShareVueHIEProvisioning@stjoe.org). Such



ST. JOSEPH HEALTH SYSTEM

<b>DIVISION:</b>	Health Information Exchange (HIE)
<b>LAST DATE REVISED: LAST DATE REVIEWED:</b>	04/27/2021
<b>ORIGINAL DATE ADOPTED:</b>	04/27/2021
<b>PAGE NUMBER:</b>	02/09/2016
<b>POLICY AND PROCEDURE #</b>	4 of 17
<b>APPROVED BY:</b>	HIE 2.0 HIE Governance

## HEALTH INFORMATION EXCHANGE

Authorized User access request form shall be completed three (3) days in advance of an anticipated additional Authorized User or within forty-eight (48) hours of such change if advance notice is not possible. This includes locums' tenens providers.

Participants shall not request access for any employee or agent whose access to the Participant's EHR System or SJH HIE has previously been terminated for privacy-related non-compliance. See below regarding "Approval or Denial of Request for an Authorized User."

Participant shall request administrative level or clinical level access to Authorized Users based on job roles (such as system administrators). Requests for Authorized User access must be for the least amount of access required to successfully fulfill their job requirements.

Approval or Denial of Request for an Authorized User: For security and privacy compliance reasons, SJHS may deny a request for access to the Clinical Portal if the employee or agent has had access terminated for noncompliance with this Policy or noncompliance with HIPAA or other state or federal privacy laws.


Training Requirements: Participants may request training for Authorized Users from SJHS by contacting HIE Department at (844) 256-4HIE (4443).

Ongoing Training Requirements: SJHS may, from time to time, require additional training associated with updates or upgrades to the Clinical Portal or related to compliance issues. Participants shall ensure that their Authorized Users timely undergo any such additional training.

Participants' HIPAA Training Obligations: All training provided by SJHS shall be in addition to, and not a substitute for, the HIPAA Privacy and Security training that Participants are obligated by HIPAA to provide their Workforce Members, including Authorized Users.

Issuance of Unique User Identification and Password: SJHS will only issue a Unique User Identification and password to access the Clinical Portal to any Authorized User once he/she has completed any required initial training related to the Clinical Portal and signed a User Access and Confidentiality Statement. Each executed User Access and Confidentiality Statement shall be forwarded to SJHS and Participants shall retain a copy of executed User Access for their records. Participants are responsible for ensuring that Authorized Users do not allow anyone else to use their Unique User Identifications and passwords to access the Clinical Portal.

Revocation or Modification of Authorized Users: To revoke or modify an Authorized User's access rights to the Clinical Portal, an authorized representative of the Participant must complete and submit an Authorized

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>5 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

User access request form via fax or email to the [ShareVueHIEProvisioning@stjoe.org](mailto:ShareVueHIEProvisioning@stjoe.org) and/or IT Service Desk at AskIT@stjoe.org within two (2) days of an anticipated revocation of, or modification to, an Authorized User’s access, or within twenty four (24) hours of such change if advance notice is not possible. Participants shall be responsible for informing the HIE Department and/or IT Service Desk if an Authorized User’s access rights are being terminated or otherwise revoked or modified due to noncompliance with this Policy, or HIPAA or other applicable laws. The IT Service Desk may reasonably deny a subsequent request from any Participant to provide access to the Clinical Portal to an individual whose access rights were previously so terminated, revoked or modified. See “Authorized User and Employee/Contractor Sanctions” below related to SJHS’s right to revoke an Authorized User’s access to the Clinical Portal.


**4.4 Patient Complaints and Potential Privacy Breaches**

To ensure accurate and consistent communications regarding complaints associated with or otherwise connected to the SJH HIE, Participants will notify the SJHS Chief Compliance/Privacy Officer at 714-381-4804, or by calling the SJH Compliance Hotline at 866-913-0275 within five (5) business days of receiving a patient complaint involving the SJH HIE. However, Participants shall be responsible for investigating all privacy-related complaints that they receive from Patients that relate strictly to the Participant’s EHR System or Participant’s non-SJH HIE related operations, pursuant to Participants’ own internal policies on handling complaints and Breach Investigations. In the event that a Patient complaint relates to a potential Breach involving the exchange of Health Information through the SJH HIE, use of the Clinical Portal, or integrity of the SJH HIE, then the “Breach Response” requirements set forth below shall be followed.

**4.5 Consent**

The PSJH HIE will operate on an opt-out consent model enterprise wide for all PSJH facilities in California, Alaska, Montana, Oregon, Texas, Washington hospitals and community connect practices Specific procedures related to SJHS’s operationalizing Patient consent are set forth in the SJH HIE Consent Policy and Procedure.

This means that a Patient’s Health Information will be made available for

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b>  <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>6 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

exchange through the SJH HIE, unless the Patient “opts-out.” If Patients desire to opt-out of allowing their PHI to be shared via the PSJH HIE, Participants shall provide such Patients with the PSJH HIE flyer and direct them to <https://www.provshare.org> or to the toll-free number at (833) 990-1900.

Because a patient’s affirmative written consent is not obtained for the sharing of all EHI, due to legal, technical, and administrative constraints, the SJH HIE may filter and not exchange certain types of Health Information that are considered sensitive or which are specially protected by applicable law, including but not limited to, HIV test results, some mental/behavioral health and substance use disorder records, and genetic/hereditary test results


**4.6 Connecting to Other Health Information Exchanges**

The SJH HIE may connect to and allow the electronic exchange of Health Information with other health information exchanges. The SJH HIE may make Health Information available to other health information exchanges and their participants, for Treatment, Payment, and Health Care Operations activities; however, such disclosures by the SJH HIE to another health information exchange will only be permitted in accordance with applicable law and due to legal, technical, and administrative constraints, Health Information that is disclosed by the SJH HIE will not include HIV test results, some mental/behavioral health records and substance use disorder records, and genetic/hereditary test results.

**4.7 Request for Restrictions of PHI Maintained on the SJHHIE**

Participants shall respond to requests from Patients for restrictions on the Uses and Disclosures of their PHI in accordance with Participants’ own internal policies and procedures related to requested restrictions involving PHI maintained in the Participant’s EHR System. However, as a matter of policy due to technological constraints, Participants shall not agree to Patients’ requests for restrictions on Disclosures which would either: (i) prohibit Participant from being a SJH HIE Data Provider; or (ii) restrict the disclosure of PHI to other Participants (or just one Participant). Despite the foregoing, if a Participant has agreed to a requested restriction, then the Participant shall be responsible for ensuring that it does not make PHI that is subject to the agreed upon restriction available to the SJH HIE in violation of the agreed to restriction.

Participants must comply with Patients’ requests to restrict Disclosures of

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 7 of 17 HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

PHI to Patients’ health plans when the PHI pertains to a health care item or service that has been paid in full by a requesting Patient or someone other than the health plan at issue, and Disclosures are for Payment or Health Care Operations purposes and not otherwise Required by Law (“Required Restriction”). If a Required Restriction is requested, then the Participant shall be responsible for ensuring that it does not make PHI that is subject to the Required Restriction available to the SJH HIE in violation of the Required Restriction.

**4.8 Request for Confidential Communications of PHI Maintained on the SJHIE**

Requests from Patients for confidential communications of PHI do not impact the SJH HIE and Participants shall follow their own internal policies and procedures related to responding to and accommodating such requests.


**4.9 Defining the Legal Medical Record and the Designated Record Set**

Related strictly to PHI that is maintained by the SJH HIE, each Participant’s own defined Legal Medical Record and Designated Record Set may only include information maintained on the Participant’s EHR System and information accessed through the SJH HIE that is relied upon in treating a Patient; not all information that may be available for access by the Participant through the SJH HIE (either via Bi-Directional Exchange or the Clinical Portal) should be included in the Participant’s defined Legal Medical Record or Designated Record Set.

**4.10 Release of Information to Third Parties**

When third parties request Participants to produce PHI or medical records of Patients, no Participant may use the SJH HIE in responding to the third-party request. Only information or records maintained by the Participant on the Participant’s EHR System may be provided in response to a third-party request.

1. Notice for Subpoenas, Court Orders and other Legal Process: If a subpoena or court order or other legal process directs a Participant to produce its “Legal Medical Record” or otherwise directs a Participant to produce Health Information that is accessible through the SJH HIE, but for which the Participant is not the originating Data Provider, the Participant must notify the requestor that its response to the subpoena or court order does not include Health Information that is accessible through the SJH HIE that is originated by other Data

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 8 of 17 HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

Providers and the requestor need to obtain such records from the originating Data Provider.

2. Other Releases to Third Parties: Disclosures of records from the SJH HIE for which Participant was not the originating Data Provider for any other purposes, such as for Research, Fundraising, Marketing, or for other purposes permitted without Patient Authorization at 45 C.F.R. 164.510 and 164.512 are not permitted. The purpose of this limitation is to ensure compliance with Applicable Law.

This section does not apply to Patients’ requests for access to their own PHI. See “Patients’ Right to Access Designated Record Sets Maintained by the SJH HIE” below.


**4.11 Patients’ Right to Access or Obtain Copy of PHI Accessible Through the SJH HIE**

If a Participant receives a request from a Patient for access to, or a copy of, PHI that is accessible through the SJH HIE, the Participant shall respond to the request in accordance with its own internal policies related to a Patient’s right to access or obtain a copy of his or her PHI, provided however, the Participant shall only provide the Patient (or designee) with access to, or a copy of, PHI that the Participant provided to the SJH HIE as a Data Provider. When responding to such an access request, a Participant shall explain to the Patient that the access or copies it has provided do not include any of the Patient’s Health Information that is accessible through the SJH HIE, but that was originally created by another Data Provider, and that to receive access to such Health Information, the Patient needs to contact the other Data Provider directly.

**4.12 Patients’ Right to Amend the PHI Accessible Through the SJH HIE**

If a Participant receives a request for amendment to PHI from a Patient related to PHI that is accessible through the SJH HIE and the Participant provided the PHI to the SJH HIE as a Data Provider, the Participant shall determine whether to grant or deny the request in accordance with its own internal policies related to a Patient’s right to amend his or her PHI. If a Participant receives a request for amendment to PHI from a Patient related to PHI that is accessible through the SJH HIE and the Participant was not the Data Provider, the Participant shall direct the Patient to make the request to the originating Data Provider of the PHI, to the extent that the Participant has knowledge of the originating Data Provider.



 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>9 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

**4.13 Accounting of Disclosures of PHI Made Through the SJH HIE**

If a Participant receives a request for an accounting of disclosures of PHI from a Patient, the Participant shall respond to the Patient’s request in accordance with the Participant’s own internal policies related to a Patient’s right to request an accounting of disclosures. SJHS will cooperate with the Participant in responding to the request by providing the Participant with all necessary, in accordance with and as set forth in the Business Associate Agreement entered between SJHS and Participant.

**4.14 Audits**

SJHS will conduct audits of the SJH HIE. Participants are also required to audit access to the SJH HIE by their Authorized Users and other employees, agents and contractors. Such audits shall be conducted as follows:


- Practice Audits: Participants shall run monthly audit reports to monitor appropriateness of access to the Clinical Portal, including instances where information was accessed related to a Patient not receiving treatment from the Participant/Authorized User.
- Proactive Audits: HIE department shall run quarterly audits of “Break the Glass” occurrences.
- Reactive Audits: PSJH Compliance and/or HIE Department shall conduct audits in the event there is a potential Breach or at the request of PSJH Compliance.

Any inappropriate access to the SJH HIE that is identified through an audit shall be reported pursuant to the requirements in the “Breach Response” section below.

**4.15 User ID/Password Management**

All Authorized Users must follow the following password-related processes when logging into the Clinical Portal:

- Passwords may not be visible on the screen as they are keyed during the logon process, or at any other time.
- Authorized Users shall not be permitted to compose a password with one- character or keyboard scales.
- Passwords must be a minimum of eight -(8) characters and include at least one of each the following requirements: upper case letter, lower-case letter, number and special character.

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>10 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

- Users are disabled after (5) failed login attempts and must contact PSJH Service Desk to re-enable the user account.
- There must be 5 generations for password history which means that an Authorized User shall be unable to input any of the last 5 passwords that they have previously used as their new password upon a required or voluntary change of password.

The User IDs of Authorized Users that have not logged into the Clinical Portal for a period over 90 days shall automatically be disabled.


Authorized Users shall be automatically logged off of the Clinical Portal after 15 minutes of inactivity. The termination shall remain in effect until the Authorized User reestablishes access using appropriate identification and log-in processes.

Each Participant must implement similar requirements for Participant’s EHR System that is connected to the SJH HIE for Bi-Directional Exchange transactions.

**4.16 Breach Response**

If a Participant discovers, or receives a complaint related to, a suspected impermissible acquisition, access, use or disclosure of PHI involving the SJH HIE, the Participant shall promptly report the discovery or complaint to the SJHS Integrity Hotline at 1-888-294-8455 or by logging onto [www.psjhealth.org/integrityonline](http://www.psjhealth.org/integrityonline), within twenty-four (24) hours. The report shall include the identification of the Authorized User or Participant involved in the suspected impermissible acquisition, access, use, or disclosure, the identity of the complainant (when applicable), and a brief description of what happened, including the date of the suspected impermissible acquisition, access, use, or disclosure, and the date of discovery of the suspected impermissible acquisition, access, use, or disclosure. Similarly, if SJHS, as the business associate of the Participants, discovers a suspected impermissible acquisition, access, use or disclosure of PHI made through the SJH HIE, SJHS will notify the relevant Participants in accordance with the terms of the relevant Business Associate Agreement.

Following the receipt of notice of a suspected impermissible acquisition, access, use or disclosure of PHI involving the SJH HIE, the relevant Participants, including SJHS, must work together to investigate the event and determine if it is a Breach such that legally required notifications are necessary. In the event that a Breach is substantiated by SJHS, the relevant

 <b>ST. JOSEPH HEALTH SYSTEM</b>	<b>DIVISION:</b> <b>LAST DATE REVISED: LAST DATE REVIEWED:</b> <b>ORIGINAL DATE ADOPTED:</b> <b>PAGE NUMBER:</b> <b>POLICY AND PROCEDURE #</b> <b>APPROVED BY:</b>	Health Information Exchange (HIE) 04/27/2021 04/27/2021 02/09/2016 <b>11 of 17</b> HIE 2.0 HIE Governance
<b>HEALTH INFORMATION EXCHANGE</b>		

Participants shall cooperate with SJHS in notifying affected Patients in order to ensure that affected Patients do not receive more than one Breach

notification per incident. All Participants must cooperate with SJHS in taking steps to correct any weaknesses related to this Policy or the operations of the SJH HIE that are identified as a result of a suspected impermissible acquisition, access, use or disclosure or a Breach.

**4.17 Authorized User and Employee/Contractor Sanctions**

Participants shall impose appropriate sanctions upon Authorized Users and any employees, agents, or contractors that fail to comply with this Policy, HIPAA, or applicable state or other federal privacy laws when accessing or using the SJH HIE. In addition to the foregoing, SJHS, as the host of the SJH HIE, has the right to revoke or modify any Authorized Users’ access to the Clinical Portal for failure to comply with this Policy, HIPAA or other applicable state or federal privacy laws when accessing the SJH HIE.

**4.18 Participant Dispute Resolution**

Participants shall work together collaboratively and in good faith to resolve disputes between and amongst themselves related to the SJH HIE. SJHS will help to facilitate the resolution of all disputes between Participants related to the SJH HIE.

**4.19 No Information Blocking Permitted**

The SJH HIE and its Participants must comply with the requirements of the Information Blocking Rule, to the extent that the Participant is an Actor (“Participant Actors”), and the SJH HIE and such Participant Actors shall not engage in practices that violate the Information Blocking Rule in connection with the SJH HIE. This policy is not intended to prevent the SJH HIE or Participant Actors from engaging in activities that are Required By Law or that fall within a Safe Harbor.

The SJH HIE and its Participant Actors are each independently responsible for identifying, assessing, and determining whether its own practices implicate the prohibition on Information Blocking, are Required By Law, or qualify for a Safe Harbor, as well as for monitoring and enforcing their own compliance with the Information Blocking Rule in connection with participation in the SJH HIE.



ST. JOSEPH HEALTH SYSTEM

**DIVISION:**

Health Information Exchange (HIE)  
04/27/2021  
04/27/2021  
02/09/2016  
12 of 17  
HIE 2.0  
HIE Governance

**LAST DATE REVISED: LAST**

**DATE REVIEWED:**

**ORIGINAL DATE ADOPTED:**

**PAGE NUMBER:**

**POLICY AND PROCEDURE #**

**APPROVED BY:**

**HEALTH INFORMATION EXCHANGE**

If a Participant Actor reasonably believes that the SJH HIE or another Participant Actor is violating the Information Blocking Rule in connection with its participation in the SJH HIE, it should promptly notify the SJH HIE. The SJH HIE will determine the best approach for addressing the complaint, which may include requesting that the other Participant Actor respond to the allegation or taking other appropriate action depending on the facts and circumstances surrounding the complaint.

Participant Actors shall cooperate with the SJH HIE in any investigation into a complaint of Information Blocking, including providing, upon reasonable request of the SJH HIE an explanation of the practice alleged to constitute Information Blocking and/or producing any necessary or relevant documentation to support application of a Safe Harbor.

**5 DEFINITIONS**

<b>Term</b>	<b>Definition</b>
Actor	A health care provider (as defined in 42 U.S.C. § 300jj), a developer of certified health IT (CHIT Developer) or a health information network (HIN)/health information exchange (HIE), all as defined by the Information Blocking Rule at 45 C.F.R. § 171.102.
Authorized Users	The health care providers and other individuals identified by a Participant who are: (a) clinical personnel employed by, are shareholders or members of, or are under contract with or have medical staff membership at, the Participant to provide clinical care on behalf of the Participant; and (b) employees of the Participant who provide administrative support to the Participant and who require access to Health Information through the SJH HIE to perform their duties on behalf of the Participant. All Authorized Users that will be using the Clinical Portal must sign a User Access and Confidentiality Statement.
Bi-Directional Exchange	The exchange of Health Information through an interface between the SJH HIE and a Participant’s EHR System in a query and response format, such that the Participant is both a Data Provider and Data Recipient through the single interface.



ST. JOSEPH HEALTH SYSTEM

**DIVISION:**

**LAST DATE REVISED: LAST**

**DATE REVIEWED:**

**ORIGINAL DATE ADOPTED:**

**PAGE NUMBER:**

**POLICY AND PROCEDURE #**

**APPROVED BY:**

Health Information Exchange (HIE)

04/27/2021

04/27/2021

02/09/2016

13 of 17

HIE 2.0

HIE Governance

**HEALTH INFORMATION EXCHANGE**

Breach	The impermissible or unauthorized access use or disclosure of Health Information. "Unauthorized" means the inappropriate access, review, or viewing of Health Information without a direct need to view the information for medical diagnosis, Treatment, or other lawful use as permitted by applicable law.
Breach Notification Rule	The Notification in the Case of Breach of Unsecured Protected Health Information regulations at 45 C.F.R. Part 164, Subpart D.
Business Associate	Any party that acts as a "business associate" of SJHS or a Participant, as defined in 45 C.F.R. § 160.103.
Clinical Portal	The web-based portal through which a Participant that is a Data Recipient, or such Participant's Authorized Users, can access Health Information in the SJH HIE.
Data Provider	A Participant that provides Health Information to the SJH HIE.
Data Recipient	A Participant (and its Authorized Users) that receive Health Information from the SJH HIE, either via Bi-Directional Exchange or the Clinical Portal.
Designated Record Set	A group of records maintained by or for a Participant that is: (1) the medical records and billing records about Patients maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the Participant to make decisions about Patients.
Electronic Health Information or EHI	Electronic PHI contained in a Designated Record Set, regardless of whether the group of records are used or maintained by or for a covered entity, as those terms are defined by HIPAA. EHI specifically excludes psychotherapy notes or information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding. EHI also excludes data de-identified in accordance with the HIPAA.
Health Care Operations	The same meaning as the term "health care operations" set forth at 45 C.F.R. § 164.501.
Health Information	The health-related information of a Patient that is disclosed and accessed through the SJH HIE for Permitted Uses. For purposes of this Policy, all Health Information will be considered Protected Health Information.



ST. JOSEPH HEALTH SYSTEM

**DIVISION:**

Health Information Exchange (HIE)  
04/27/2021  
04/27/2021  
02/09/2016  
14 of 17  
HIE 2.0  
HIE Governance

**LAST DATE REVISED: LAST**

**DATE REVIEWED:**

**ORIGINAL DATE ADOPTED:**

**PAGE NUMBER:**

**POLICY AND PROCEDURE #**

**APPROVED BY:**

**HEALTH INFORMATION EXCHANGE**

HIPAA	The Health Insurance Portability and Accountability Act of 1996, specifically including the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164) as amended by the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”) and any further amendments, modification, or renumbering thereof.
Information Blocking	Practices (i.e., acts or omissions) that are likely to prevent, materially discourage or otherwise inhibit (i.e., to interfere with) the access, exchange or use of Electronic Health Information (EHI), including: <ul style="list-style-type: none"> <li>• The ability or means necessary to make EHI available for exchange or use (i.e., access to EHI);</li> <li>• The ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks (i.e., exchange of EHI); and/or</li> <li>• The ability for EHI, once accessed or exchanged, to be understood and acted upon (i.e., use of EHI).</li> </ul>
Participant	A party that has signed a Participation Agreement with SJHS to act as a Data Provider and/or a Data Recipient.
Participant’s EHR System	The electronic health record system used by a Participant to maintain the Participant’s Patient medical records.
Participation Agreement	A legally binding agreement between SJHS and a Participant for the use of the SJH HIE.
Patient	The person who is the subject of PHI.
Payment	The same meaning as the term “payment” set forth at 45 C.F.R. § 164.501.
Privacy Rule	The regulations at 45 C.F.R. Part 160 and 164, Subparts A and E, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.



ST. JOSEPH HEALTH SYSTEM

**DIVISION:**

Health Information Exchange (HIE)  
04/27/2021  
04/27/2021  
02/09/2016  
15 of 17  
HIE 2.0  
HIE Governance

**LAST DATE REVISED: LAST**

**DATE REVIEWED:**

**ORIGINAL DATE ADOPTED:**

**PAGE NUMBER:**

**POLICY AND PROCEDURE #**

**APPROVED BY:**

**HEALTH INFORMATION EXCHANGE**

Protected Health Information or PHI	Any information, whether oral or recorded in any form or medium, that is created or received by a covered entity, including demographic information, that (a) relates to the past, present, or future physical or mental health or condition of a Patient; the provision of health care to a Patient, or the past, present, or future payment for the provision of health care to a Patient; (b) identifies the Patient (or for which there is a reasonable basis for believing that the information can be used to identify the individual.
Required By Law	A practice that is explicitly required by State or Federal law, including statutes, regulations, court orders, binding administrative decisions or settlements (including FTC or EEOC), as well as tribal law (as applicable). Required by Law does not mean practices permitted by law or engaged in pursuant to a law (such as privacy laws that require an individual's consent or authorization prior to disclosing EHI to the requestor).
Safe Harbor	<p>The regulatory exceptions to the Information Blocking Rule, set forth at 42 C.F.R. §§ 171.200 through 171.303, which are identified as reasonable and necessary activities that do not constitute Information Blocking. The following is a general list of the Safe Harbors:</p> <ul style="list-style-type: none"> <li>• Preventing Harm Exception</li> <li>• Privacy Exception</li> <li>• Security Exception</li> <li>• Content and Manner Exception</li> <li>• Infeasibility Exception</li> <li>• Fees Exception</li> <li>• Licensing Exception</li> <li>• Health IT Performance Exception</li> </ul> <p>All of the regulatory conditions must be met in order for a Safe Harbor to apply.</p>
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.



ST. JOSEPH HEALTH SYSTEM

**DIVISION:**

**LAST DATE REVISED: LAST**

**DATE REVIEWED:**

**ORIGINAL DATE ADOPTED:**

**PAGE NUMBER:**

**POLICY AND PROCEDURE #**

**APPROVED BY:**

Health Information Exchange (HIE)

04/27/2021

04/27/2021

02/09/2016

16 of 17

HIE 2.0

HIE Governance

**HEALTH INFORMATION EXCHANGE**

Security Rule	The Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and 164, Subparts A and C.
SJH HIE	SJHS’s systems, devices, mechanisms and infrastructure to facilitate the electronic movement of Patient Health Information between and among Participants. The SJH HIE includes all interfaces used by Data Providers to contribute Health Information to the SJH HIE, all interfaces necessary to conduct Bi-Directional Exchange, and the Clinical Portal.
Subcontractor	Any downstream entity who has been delegated a function, an activity or a service that a Business Associate has agreed to perform, on behalf of a Participant or another Business Associate.
Treatment	The same meaning as the term “treatment” set forth at 45 C.F.R. § 164.501.
Workforce	Employees, volunteers, trainees, and other persons whose conduct in the performance of work for a Participant is under the direct control of the Participant, whether they are paid by the Participant.



## **6 ATTACHMENTS**

1. User Access and Confidentiality Statement