Contents

Scope:

This policy applies to the not-for-profit, non-profit entities of Providence and its Affiliates (collectively known as "Providence") and their workforce members (caregivers, volunteers, trainees, interns, apprentices, students), independent contractors, vendors and all other individuals working at the ministry, whether they are paid by or under the direct control of the facility; employees of affiliated organizations (collectively, "workforce members"). Where a Providence organization is not wholly or majority owned, exceptions may apply.

☒ Yes ☐ No Is this policy applicable to Providence Global Center caregivers?

This is a management level policy reviewed and recommended by the Policy Advisory Committee to consider for approval by senior leadership which includes vetting by Executive Council with final approval by the President, Chief Executive Officer, or appropriate delegate.

Purpose:

To establish policies and procedures related to the operation of and participation in the SJH HIE (defined below). This SJH HIE Policy ("Policy") serves as a guide to help Participants and SJH HIE Workforce Members understand their obligations related to the SJH HIE and ensure compliance with all applicable laws and regulations.

Definitions:

Term	Definition
Actor	A health care provider, a developer of certified health IT, health information network, or health information exchange, all as defined by the Information Blocking Rule.
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 Patient Health Information through the SJH HIE to perform their duties on behalf of the Participant.

Bi-Directional Exchange	The exchange of Patient 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.
Business Associate	Any party that acts as a "business associate" of Providence 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 a Participant's Authorized Users, access Patient Health Information in the SJH HIE.
Data Provider	A Participant that provides Patient Health Information to the SJH HIE.
Data Recipient	A Participant (and its Authorized Users) that receives Patient 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.
Health Care Operations	The same meaning as the term "health care operations" set forth at 45 C.F.R. § 164.501.
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 Rule	Collectively, 42 U.S.C. § 300j-52 and its implementing regulations.

Patient Health Information	The health-related information of a Patient that is disclosed and accessed through the SJH HIE. For purposes of this Policy, all Patient Health Information is considered PHI.
Participant	An individual or entity that has entered into a legally binding agreement with Providence to participate in the SJH HIE 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.
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.
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.
Security Incident	Any attempted or impermissible or unauthorized access, use, modification, destruction or disclosure of Patient Health Information. "Unauthorized" means the inappropriate access, review, or viewing of Patient Health Information without a direct need to view the information for medical diagnosis, Treatment, or other lawful use as permitted by applicable law.
SJH HIE	Providence's systems, devices, mechanisms and infrastructure to facilitate the electronic movement of Patient Health Information between and among Participants on behalf of the SJH HIE. 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.
Treatment	The same meaning as the term "treatment" set forth at 45 C.F.R. § 164.501.

Policy:

It is the policy of Providence, as well as persons or entities that contract with Providence, including Participants, when applicable, to comply with all federal laws and regulations, including HIPAA, related to the access and exchange of Patient Health Information and the operation of, and participation in, the SJH HIE and Clinical Portal operated by Providence.

Procedures:

1. **Compliance with HIPAA; Permissible Use of the SJH HIE**

   Participant shall fully comply with HIPAA when exchanging and accessing Patient Health Information through the SJH HIE. Participant shall be responsible for ensuring it maintains all appropriate policies, procedures and measures necessary to comply with such requirements, including without limitation, privacy and security training, appropriate technical controls when accessing the SJH HIE, audit control processes, and other measures to detect Security Incidents involving the SJH HIE.

   Participant and its Authorized Users are only permitted to use the Clinical Portal to access Patient Health Information for Patients with whom the accessing Participant or its Authorized Users have a Treatment relationship. If a Treatment relationship does not exist, Authorized Users must break the glass 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.

   Patient 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 Patient 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 Patient 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 all Patient Health Information due to the HIPAA minimum necessary requirements, state limitations, and technical constraints.

   Patient 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, if the Patient who is the subject of the Patient Health Information is matched between the SJH HIE and the Participant using the enterprise master patient index.

   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.

2. Notice of Privacy Practices

Participant is encouraged to utilize the following specific language in its Notice of Privacy Practices to inform Patients about its 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 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 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, 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 minimum, 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 Patient 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. Participant must also ensure that it adequately informs Patients of their right to opt-out of the SJH HIE or obtain a Patient's opt-in consent, when required by law.

The SJH HIE may provide Patient education materials related to the SJH HIE. Participant shall ensure that Patients receive all patient education materials.

3. Clinical Portal Authorized Users

a. Identification of Authorized Users:

Participant 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, Participant must complete an Authorized User Access Request Form and submit it to ShareVueHIEProvisioning@stjoe.org.

The Authorized User Access Request Form must 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.

Participant 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, and the SJH HIE may deny a request for access to the Clinical Portal if the employee or agent has had access terminated for noncompliance with this Policy, HIPAA, or other state or federal privacy laws.

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 fulfil their job requirements.

b. SJH HIE Training:

Participant may request training for Authorized Users from the SJH HIE by contacting the SJH HIE Department at (844) 256-4HIE (4443).

The SJH HIE may, from time to time, require additional training associated with updates or upgrades to the Clinical Portal or related to compliance issues. Participant shall ensure that its Authorized Users timely undergo any such additional training.

All SJH HIE training shall be in addition to, and not a substitute for, any training that Participant is obligated to provide to its employees, agents and contractors under HIPAA, including its Authorized Users.

c. Issuance of Unique User Identification and Password:

All Authorized Users must sign the User Access and Confidentiality Statement, which is attached to this Policy. The SJH HIE will only issue a unique user identification and password to access the Clinical Portal to an Authorized User once the Authorized User has completed all 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 the SJH HIE. Participant shall retain a copy of the executed User Access and Confidentiality Statements for its records. Participant is responsible for ensuring that Authorized Users do not allow anyone else to use their unique user identifications and passwords to access the Clinical Portal.

d. Revocation or Modification of Authorized Users:

To revoke or modify an Authorized User's access rights to the Clinical Portal, Participant's authorized representative must complete and submit an Authorized User Access Request Form via fax or email to ShareVueHIEProvisioning@stjoe.org and/or the 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. Participant shall be responsible for informing the SJH 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, 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.

Participant shall impose appropriate sanctions upon Authorized Users and any of its 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, 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. Patient Complaints

To ensure accurate and consistent communications regarding complaints associated with or otherwise connected to the SJH HIE, Participant will notify the Providence Chief Compliance/Privacy Officer at 714-381-4804, or by calling the Providence Compliance Hotline at 866-913-0275 within five (5) business days of receiving a Patient complaint involving the SJH HIE. Participant shall be responsible for investigating all privacy-related complaints that it receives from Patients that relate strictly to the Participant's EHR System or Participant's non-SJH HIE related operations, pursuant to Participant's own internal policies. In the event that a Patient complaint relates to a potential Security Incident involving the exchange of Patient Health Information through the SJH HIE, use of the Clinical Portal, or integrity of the SJH HIE, Participant will follow the "Security Incident" requirements set forth below.

5. Security Incident Response

If Participant discovers, or receives a complaint related to a Security Incident, the Participant shall promptly report the discovery or complaint to the Providence Integrity Hotline at 1-888-294-8455 or by logging onto 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 Security Incident, the identity of the complainant (when applicable), and a brief description of what happened, including the date of the suspected Security Incident, and the date of discovery of the suspected Security Incident.

If the SJH HIE discovers a Security Incident, it will notify the relevant Participant in accordance with the terms of the relevant Business Associate Agreement.

Following the receipt of notice of a suspected Security Incident, the relevant Participant and SJH HIE will work together to investigate the event and determine if it is a Security Incident such that legally required notifications are necessary. In the event that a Security

Incident is substantiated by Providence, Participant shall cooperate with Providence in notifying affected Patients to ensure that affected Patients do not receive more than one notification per incident. All Participants must cooperate with the SJH HIE 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 Security Incident.

6. Consent

The SJH HIE will operate on an opt-out consent model enterprise-wide for all Providence facilities, hospitals, and community connect practices in California, Alaska, Montana, Oregon, Texas, and Washington. Specific procedures related to the SJH HIE's's operationalizing of 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 exchange through the SJH HIE, unless the Patient "opts-out." If a Patient desires to opt-out of allowing his or her PHI to be shared via the SJH HIE, Participant shall provide the Patient with the SJH HIE flyer and direct the Patient 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 Patient Health Information due to legal, technical, and administrative constraints, the SJH HIE may filter and not exchange certain types of Patient Health Information that is considered sensitive or which is 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.

7. Connecting to Other Health Information Exchanges

The SJH HIE may connect to and allow for the exchange of Patient Health Information with other health information exchanges. The SJH HIE may make Patient 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 subject to legal, technical, and administrative constraints. Patient Health Information 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.

8. Request for Restrictions of PHI Maintained on the SJH HIE

For PHI maintained on Participant's EHR System, Participant shall respond to Patient requests for restrictions on the use and disclosure of PHI in accordance with Participant's internal policies and procedures. However, due to technological constraints, Participant shall not agree to Patients' requests for restrictions on uses and disclosures which would either: (i) prohibit Participant from being a SJH HIE Data Provider; or (ii) restrict the disclosure of Patient Health Information to other Participants (or just one Participant).

Despite the foregoing, if a Participant has agreed to a requested restriction, 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 restriction.

Participant must comply with Patients' requests to restrict uses and disclosures of 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 uses 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 is 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.

9. Request for Confidential Communications of PHI Maintained on the SJH HIE

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

10. 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 on 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.

11. Release of Information to Third Parties

When third parties request Participant produce PHI or Patient medical records, Participant may not 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.

a. Notice for Subpoenas, Court Orders and other Legal Process:

If a subpoena, court order, or other legal process directs a Participant to produce its legal medical record, or otherwise directs a Participant to produce PHI accessible through the SJH HIE, but for which the Participant is not the originating Data Provider, Participant must notify the requestor that its response does not include PHI accessible through the SJH HIE that was originated by other Data Providers. The response must also state that the requestor must obtain such records from the originating Data Provider.

b. 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.

This section does not apply to Patients' requests for access to their own PHI, which is discussed below.

12. Patient Rights Regarding PHI Accessible Through the SJH HIE

If a Participant receives a Patient request to access, copy, or amend PHI, or a request for an accounting of disclosures, and the Participant provided the PHI to the SJH HIE as a Data Provider, the Participant shall respond to the request in accordance with its own internal policies, subject to the following:

- 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. Participant shall explain to the Patient that the PHI provided does not include any PHI from the SJH HIE that was provided by another Data Provider and that, to receive access to such PHI, the Patient must contact the other Data Provider directly.
- 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.

The SJH HIE will cooperate with the Participant in responding to a Patient request for accounting of disclosures by providing the Participant with all necessary information, in accordance with and as set forth in the Business Associate Agreement entered between Providence and Participant.

13. Audits

Providence will conduct audits of the SJH HIE. Participant is also required to audit access to the SJH HIE by its Authorized Users and other employees, agents and contractors. Such audits shall be conducted as follows:

- **Practice Audits:** Participant 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:** The SJH HIE department shall run quarterly audits of break the glass occurrences.
- **Reactive Audits:** Providence Compliance and/or the SJH HIE Department shall conduct audits in the event there is a potential Security Incident or at the request of Providence Compliance.

Any inappropriate access to the SJH HIE that is identified through an audit shall be reported pursuant to the requirements in the Security Incident section above.

14. Participant Dispute Resolution

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

15. Compliance with the Information Blocking Rule

To the extent Participant is an Actor, the SJH HIE and its Participant Actors must comply with the requirements of the Information Blocking Rule. The SJH HIE and Participant Actors shall not engage in practices that violate the Information Blocking Rule. 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 regulatory exception to the Information Blocking Rule.

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 or are required by law, and must monitor and enforce their own compliance with the Information Blocking Rule in connection with participation in the SJH HIE.

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 (i) requesting that the other Participant Actor respond to the allegation, or (ii) taking other appropriate actions 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 regulatory exception to the Information Blocking Rule.

Requirements:

None.

References:

None.

Attachments:

1. User Access and Confidentiality Statement
2. Authorized User Access Request Form (www.sharevue.org; User Request Forms 1 & 2)