

VERSION DATED AUGUST 2013/TEXAS AND CALIFORNIA

This Business Associate Addendum ("Addendum") supplements and is made a part of the service contract(s) ("Contract") by and between St. Joseph Health System ("SJH") acting on behalf of its ministries, all of which are Covered Entities as that term is defined herein and _____ ("Business Associate" or "BA"). This Addendum is effective as of _____ (the "Addendum Effective Date").

- A. SJH is the designated "business associate" (as defined at 45 C.F.R. Section 160.103) for the Organized Health Care Arrangement ("OHCA") in which SJH's ministries are members.
- B. SJH wishes, through its ministries, to disclose certain information to BA pursuant to the terms of the Contract, some of which may constitute Protected Health Information ("PHI") (defined below).
- C. SJH and BA intend to protect the privacy and provide for the security of PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable state and federal laws and regulations.
- D. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require SJH to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Addendum.

In consideration of the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

1. **Definitions**

- a. **Breach** shall have the meaning given to such term under HIPAA, the HIPAA Regulations and the HITECH Act, and in those states referenced in Section 2(m) herein under applicable state law.
- b. **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including 45 C.F.R. Section 160.103.
- c. **Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.
- d. **Data Aggregation** shall have the meaning given to such term under the Privacy Rule, including but not limited to, 45 C.F.R. Section 164.501.

- e. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- f. **Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.
- g. **Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.
- h. **Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- i. **HITECH Compliance Date** shall mean the date for compliance set forth in the HITECH Act or the implementation regulations thereunder.
- j. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- k. **Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. Protected Health Information includes Electronic Protected Health Information.
- l. **Protected Information** shall mean PHI provided by SJH to BA or created or received by BA on SJH's behalf.
- m. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.
- n. **Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h) and 45 C.F.R. Section 164.402.

2. **Obligations of Business Associate**

- a. **Permitted Uses.** BA shall not use Protected Information except for the purpose of performing BA's obligations under the Contract and as permitted under the Contract and Addendum. Further, BA shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by SJH. However, BA may use Protected Information (i) for the proper management and administration of BA, (ii) to carry out the legal responsibilities of BA, or (iii) for Data Aggregation purposes for the Health Care Operations of SJH.
- b. **Permitted Disclosures.** BA shall not disclose Protected Information except for the purpose of performing BA's obligations under the Contract and as permitted under the Contract and Addendum. BA shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by SJH.

However, BA may disclose Protected Information (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of SJH. If BA discloses Protected Information to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach.

- c. **Prohibited Uses and Disclosures under HITECH.** Notwithstanding any other provision in this Addendum, no later than the HITECH Compliance Date, BA shall comply with the following requirements: (i) BA shall not use or disclose Protected Information for fundraising or marketing purposes, except as provided under the Contract and consistent with the requirements of 42 U.S.C. 17936 and the Privacy Rule; (ii) BA shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates consistent with the requirements of 42 U.S.C. Section 17935(a) and the Privacy Rule; (iii) BA shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of SJH and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2) and the Privacy Rule; however, this prohibition shall not affect payment by SJH to BA for services provided pursuant to the Contract.
- d. **Appropriate Safeguards.** BA shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by the Contract or Addendum. BA further agrees to use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI. No later than the HITECH Compliance Date, BA shall comply with Subpart C of Part 164 of the Security Rule. To the extent that BA creates, maintains, receives or transmits Electronic PHI on behalf of the SJH, BA shall implement the safeguards required by this paragraph 2.d with respect to Electronic PHI.
- e. **Mitigation.** BA agrees to mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of PHI in violation of this Addendum.
- f. **Reporting of Improper Access, Use or Disclosure.** BA shall, following the discovery of any Breach of Unsecured PHI, Security Incident, as defined in the Security Rule, and/or any actual or suspected access, use or disclosure of Protected Information not permitted by the Contract and Addendum or applicable law notify SJH in writing of such breach or disclosure without unreasonable delay and in no case later than three business days after discovery. Notwithstanding the foregoing, BA and SJH acknowledge the ongoing existence and occurrence of attempted but unsuccessful Security Incidents that are trivial in nature, such as pings and port scans, and SJH acknowledges and agrees that no additional notification to SJH of such unsuccessful Security Incidents is required. However, to the extent that BA becomes aware of an unusually high number of such unsuccessful Security Incidents due to the repeated acts of a single party, BA shall notify SJH of these attempts and provide the name, if available, of said party. BA shall take prompt corrective action and any action required by applicable state or federal laws and regulations relating to such disclosure. BA agrees to pay the actual costs of SJH to provide required notifications and

any associated costs incurred by SJH, such as credit monitoring for affected patients, and including any civil or criminal monetary penalties or fines levied by any federal or state authority having jurisdiction if SJH reasonably determines that the nature of the breach warrants such measures.

- g. **Business Associate's Subcontractors and Agents.** In accordance with 45 C.F.R. Sections 164.308(b)(2) and 164.502(e)(1)(ii), BA shall ensure that any agents or subcontractors that create, receive, maintain, or transmit PHI on behalf of BA agree in writing to the same restrictions and conditions that apply to BA with respect to such PHI.
- h. **Access to Protected Information.** To the extent BA maintains a Designated Record Set on behalf of the SJH, BA shall make Protected Information maintained by BA or its agents or subcontractors in Designated Record Sets available to SJH for inspection and copying within five (5) days of a request by SJH to enable SJH to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524. No later than the HITECH Compliance Date, if BA maintains a Designated Record Set electronically, and if an individual requests an electronic copy of such information, BA must provide SJH, or the individual or person properly designated by the individual, as directed by SJH, access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by SJH and the individual. Any fee that BA may charge for such electronic copy shall not be greater than BA's labor and supply costs in responding to the request.
- i. **Amendment of PHI.** To the extent BA maintains a Designated Record Set on behalf of SJH, within thirty (30) days of receipt of a request from the SJH or an individual for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, BA or its agents or subcontractors shall make any amendments that SJH directs or agrees to in accordance with the Privacy Rule.
- j. **Accounting Rights.** Within thirty (30) days of notice by SJH of a request for an accounting of disclosures of Protected Information, BA and its agents or subcontractors shall make available to SJH the information required to provide an accounting of disclosures to enable SJH to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, and, no later than the HITECH Compliance Date, its obligations under the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c), as determined by SJH. The provisions of this subparagraph 2.j shall survive the termination of this Addendum.
- k. **Governmental Access to Records.** BA shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to SJH and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), or Secretary's designated representative, for purposes of determining SJH's, the ministries' and BA's compliance with the Privacy Rule.
- l. **Minimum Necessary.** No later than the HITECH Compliance Date, BA (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure. BA understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

- m. **Compliance with Applicable State Laws.** Both Parties acknowledge and agree that SJH has ministries located in California and Texas and the services being provided by BA may be provided to some or all of SJH's ministries located in each of those states. To the extent state law in either state is not preempted by HIPAA, BA shall comply with applicable state law protecting the access, use, disclosure and maintenance of PHI including without limitation requirements for reporting of a breach, breach notification to affected individuals and training of BA's work force. For clarification, the current applicable state laws include the following:
1. Texas
 - (i) Tex. Bus. Com. Code Ann. Section 521.001 et seq.
 - (ii) Tex. Health & Safety Code Ann. Section 181.001 et seq. and more specifically Section 181.101 (training program requirements for BA's employees) and Section 181.154 (notice to individuals if the individual's PHI is subject to electronic disclosure).
 2. California

Cal. Civil Code Section 1798.80 et seq. and Cal. Civil Code Section 56-56.07 (Confidentiality of Medical Information Act)
- n. **Delegation of Obligations.** To the extent BA is delegated to carry out SJH's obligations under the Privacy Rule, BA shall comply with the requirements of the Privacy Rule that apply to SJH in the performance of such delegated obligation.

3. Termination

- a. **Material Breach by BA.** A breach by BA of any provision of this Addendum, as determined by SJH, shall constitute a material breach of the Contract and shall provide grounds for termination of the Contract, any provision in the Contract to the contrary notwithstanding, with or without an opportunity to cure the breach. If termination of the Contract is not feasible, SJH will report the problem to the Secretary of DHHS. BA shall ensure that it maintains for itself the termination rights in this Section in any agreement it enters into with a subcontractor pursuant to section 2(g) hereof.
- b. **Material Breach by SJH.** As of the HITECH Compliance Date, pursuant to 42 U.S.C. Section 17934(b), if the BA knows of a pattern of activity or practice of the SJH that constitutes a material breach or violation of the SJH's obligations under the Contract or Addendum or other arrangement, the BA must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the BA must terminate the Contract or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS.
- c. **Effect of Termination.** Upon termination of the Contract for any reason, BA shall, at the option of SJH, return or destroy all Protected Information that BA or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by SJH, BA shall continue to extend the protections of Section 2 of this Addendum to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. If SJH elects destruction of the PHI, BA shall certify in writing to SJH that such PHI has been destroyed.

4. **Indemnification; Limitation of Liability.** To the extent permitted by law, BA shall indemnify, defend and hold harmless SJH from any and all liability, claim, lawsuit, injury, loss, expense or damage resulting from or relating to the acts or omissions of BA in connection with the representations, duties and obligations of BA under this Addendum. Any limitation of liability contained in the Contract shall not apply to the indemnification requirement of this provision. This provision shall survive the termination of the Addendum.
5. **Assistance in Litigation.** BA shall make itself and any subcontractors, employees or agents assisting BA in the performance of its obligations under the Contract or Addendum available to SJH, at no cost to SJH, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against SJH, its directors, officers or employees based upon a claim of violation of HIPAA, the HITECH Act, or other laws related to security and privacy.
6. **Amendment to Comply with Law.** The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Contract or Addendum may be required to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations, the HITECH Act, and other applicable state and federal laws and regulations relating to the security or confidentiality of PHI. Upon the compliance date of any such applicable laws and regulations, this Addendum shall automatically be amended such that this Addendum remains in compliance with such laws and regulations.
7. **No Third-Party Beneficiaries.** Nothing express or implied in the Contract or Addendum is intended to confer, nor shall anything herein confer upon any person other than SJH, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever
8. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. This Addendum and the Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the Contract shall remain in force and effect.
9. **Regulatory References.** A reference in this Addendum to a section of regulations means the section as in effect or as amended, and for which compliance is required.
10. **Identity Theft Program Compliance.** To the extent that SJH is required to comply with the final rule entitled "Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003," as promulgated and enforced by the Federal Trade Commission (16 C.F.R. Part 681) (the "Red Flags Rule") and that BA is performing an activity in connection with one or more "covered accounts," as that term is defined in the Red Flags Rule, pursuant to the Contract, BA shall establish and comply with its own reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, which shall be consistent with and no less stringent than those required under the Red Flags Rule or the policies and procedures of SJH's Red Flags Program. BA shall provide its services pursuant to the Contract in accordance with such policies and procedures. BA shall report any detected "red flags," as that term is defined in the Red Flags Rule, to SJH and shall, in cooperation with Hospital, take appropriate steps to prevent or mitigate identity theft.

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Addendum Effective Date.

SJH

BUSINESS ASSOCIATE

By: _____
Name:
Title:
Date:

By: _____
Name:
Title:
Date:

ADDENDUM “B”

WAIVER OF SJHS STANDARD HIPAA BUSINESS ASSOCIATE AGREEMENT
FORM (Rev. 10/14/13)

PLEASE ENSURE THAT THIS FORM IS COMPLETED IN ITS ENTIRETY AND THAT A COPY OF THE PROPOSED BUSINESS ASSOCIATE AGREEMENT IS ATTACHED.

Note: The purpose of this form is to help consider the risks associated with accepting Business Associate Agreement provisions that are different from the SJHS standard Business Associate Agreement provisions and to document the Ministry’s understanding of such risks. This form in no way should serve as a waiver for the complete elimination of HIPAA Business Associate Agreement provisions.

REQUEST PROCESS

Date Submitted: _____ Name/Title of Submitter: _____

Phone number of Submitter: _____ Department: _____

Direct Supervisor: _____

Executive Sponsor: _____

Name of Business Associate (vendor): _____

Scope of services/products: _____

Explain how the business associate will have access to, and/or use Protected Health Information in the provision of services/products to SJHS?

Dates/term of contract: _____

Describe other agreements that Submitter’s Ministry and SJHS had/has with this Business Associate:

Has the Business Associate refused to sign the SJHS Standard HIPAA Business Associate Agreement?

Yes _____ (If yes, please complete the remainder of this form).

No _____ (If no, do not turn in this form and use the SJHS Standard HIPAA Business Associate Agreement).

Describe in detail the circumstances for which a waiver of the SJHS Standard HIPAA Business Associate Agreement is being requested (i.e. request by Business Associate for modification of the SJHS Standard HIPAA Business Associate Agreement, request by Business Associate to use their HIPAA Business Associate Agreement, or other reason) and rationale for why a waiver should be considered.

Revisions have been requested by the Business Associate for modification to the indemnification and/or limitation of liability provisions.

If so, the revisions move the indemnification/limitation of liability provisions from the Business Associate Agreement to the underlying agreement but the same level of protection is provided in the underlying agreement.

If so, the revisions provide SJHS with a different level of protection than the standard indemnification and limitation of liability provisions. Describe requested modifications:

Business Associate has requested material modifications to provisions other than the indemnification and/or limitation of liability provisions. If so, describe requested modification:

REVIEW PROCESS

By signing below, I represent that I fully understand the risks associated with accepting HIPAA Business Associate Agreement provisions other than the SJHS standard provisions, which include but are not limited to the potential costs, fines, penalties and damages SJHS, rather than the vendor, might incur as a result of the diminished protection SJHS will receive in the event of the vendor’s impermissible use or disclosure of Protected Health Information. I further understand that it is highly recommended that I seek the input and advice of the SJHS Ministry Integrity Department or SJHS Legal Services Department prior to accepting HIPAA Business Associate Agreement provisions other than the SJHS standard provisions. By signing below, I hereby represent that I have either consulted with the SJHS Chief Compliance Officer, SJHS General Counsel, Associate General Counsel, or the Regional Compliance Director, regarding the non-standard HIPAA Business Associate Agreement provisions or have assumed the risk of not pursuing such consultation and will take responsibility for such decision.

Executive Sponsor

Date Approved

The Business Associate Agreement is for a system office contract:

President of Integrated Services

Date Approved

The Business Associate Agreement is not for a system office contract:

Ministry Chief Executive Officer

Date Approved

Keep this signed form on file with all other pertinent documentation related to the Business Associate Agreement.