

RESOLUTION AGREEMENT

I. Recitals

1. **Parties.** The Parties to this Resolution Agreement (“Agreement”) are:

A. The United States Department of Health and Human Services, Office for Civil Rights (“HHS”), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the “Privacy Rule”), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the “Security Rule”), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the “Breach Notification Rule”). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the “HIPAA Rules”) by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).

B. St. Joseph Health (“SJH”), is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. SJH is a nonprofit integrated Catholic health care delivery system sponsored by the St. Joseph Health Ministry. SJH’s comprehensive range of services includes 14 acute care hospitals, and also includes home health agencies, hospice care, outpatient services, skilled nursing facilities, community clinics and physician organizations throughout California and in parts of Texas and New Mexico. Collectively, SJH has 24,000 employees and 6,000 physicians that deliver care to more than 137,000 inpatients and 3.6 million outpatients each year.

HHS and SJH shall together be referred to herein as the “Parties.”

2. **Factual Background and Covered Conduct.** On February 14, 2012, SJH reported to the HHS Office for Civil Rights that certain files created for its participation in the meaningful use program (the “Reports”), which contained protected health information (“PHI”), were publicly accessible on the internet from February 1, 2011 until February 13, 2012 through Google and possibly other internet search engines. SJH identified that this public access was caused by a configuration within the network server related to the application to which the Reports were uploaded. The Reports were in the form of PDF files which specifically included various combinations of the following patient information: patient names; BMI; blood pressure; lab results; smoking status; diagnoses lists; medication allergies; advance directive status and demographic information (language, ethnicity, race, sex, and birth date). SJH confirmed that the breach did not include social security numbers, or any other financial data. The breach provided access to the PHI of 31,800 individuals from five of the SJH hospitals – St. Jude Medical Center, Mission Hospital, Queen of the Valley Medical Center, Santa Rosa Memorial Hospital, and Petaluma Valley Hospital. On

February 13, 2012, the application that housed the Reports was shut down and external access of the affected PHI was blocked.

HHS' investigation indicated that the following conduct occurred ("Covered Conduct"):

A. From February 1, 2011 to February 13, 2012, SJH impermissibly disclosed the PHI of 31,800 individuals. *See* 45 C.F.R. § 164.502(a).

B. SJH's use of the application to which the Reports were uploaded and the related server configuration created an environmental or operational change that affected the security of ePHI; thereby triggering SJH's Security Rule obligation to conduct a technical and nontechnical evaluation. From July 1, 2010 to July 10, 2012, SJH failed to perform an evaluation in response to this operational change; thereby compromising the security of ePHI. *See* 45 C.F.R. § 164.308(a)(8).

C. From July 1, 2010, to the present, SJH failed to satisfactorily conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the ePHI held by SJH. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).

3. **No Admission.** This Agreement is not an admission, concession, or evidence of liability by SJH or of any fact or any violation of any law, rule, or regulation, including any violation of the HIPAA Rules. This Agreement is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind, and SJH's agreement to undertake any obligation under this Agreement shall not be construed as an admission of any kind.

4. **No Concession.** This Agreement is not a concession by HHS that SJH is not in violation of the HIPAA Rules and that SJH is not liable for civil money penalties.

5. **Intention of Parties to Effect Resolution.** This Agreement is intended to resolve HHS Transaction No. 12-139105, and any possible violations of the HIPAA Rules related to the Covered Conduct specified in paragraph I.2 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

6. **Payment.** SJH agrees to pay HHS the amount of \$2,140,500.00 ("Resolution Amount"). SJH agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. **Corrective Action Plan.** SJH has entered into and agrees to comply with the Corrective Action Plan (CAP), attached as Appendix A, which is incorporated into this Agreement by reference. If SJH breaches the CAP, and fails to cure the breach as set forth in

the CAP, then SJH will be in breach of this Agreement, and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. **Release by HHS.** In consideration of and conditioned upon SJH's performance of its obligations under this Agreement, HHS releases SJH and its successors, transferees, assigns, parents, subsidiaries, members, agents, directors, officers, affiliates and employees from any claims, actions, or causes of action HHS has or may have against them under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I.2 of this Agreement. HHS does not release SJH from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. **Agreement by Released Party.** SJH shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. SJH waives all procedural rights granted under section 1128A of the Social Security Act (42 U.S.C. § 1320a-7a), 45 C.F.R. Part 160, Subpart E, and HHS Claims Collection provisions, 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. **Binding on Successors.** This Agreement is binding on SJH and its successors, heirs, transferees, and assigns.

11. **Costs.** Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. **No Additional Releases.** This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against or by any other person or entity, except as otherwise specified herein.

13. **Effect of Agreement.** This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement must be in writing and signed by both Parties.

14. **Execution of Agreement and Effective Date.** The Agreement shall become effective (*i.e.*, final and binding) on the date of signing of this Agreement and the CAP by the last signatory ("Effective Date").

15. **Tolling of Statute of Limitations.** Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money penalty ("CMP") must be imposed within six (6) years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, SJH agrees that the time between the Effective Date of this Agreement and the date this Agreement may be terminated by reason of SJH's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations


applicable to the possible violations which are the subject of this Agreement. SJH waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in paragraph I.2 that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. **Disclosure.** HHS places no restriction on the publication of the Agreement. In addition, HHS may be required to disclose material related to this Agreement to any person upon request consistent with the applicable provisions of the Freedom of Information Act, ("FOIA"), 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5; provided, however, that HHS will use its best efforts to prevent the disclosure of information, documents, and any other item produced by SJH to HHS as part of HHS's review, to the extent such items constitute trade secrets and/or confidential commercial or financial information that is exempt from turnover in response to a FOIA request under 45 C.F.R. § 5.65, or any other applicable exemption under FOIA and its implementing regulations.

17. **Execution in Counterparts.** This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

18. **Authorizations.** The individual(s) signing this Agreement on behalf of SJH represent and warrant that they are authorized by SJH to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represent and warrant that they are signing this Agreement in their official capacities and that they are authorized to execute this Agreement.

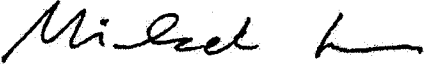
For St. Joseph Health



Annette M. Walker
Chief Executive-SJH

10-13-16
Date

For the United States Department of Health and Human Services



Michael Leoz
Regional Manager
Office for Civil Rights, Pacific Region

10-13-16
Date

Appendix A

CORRECTIVE ACTION PLAN BETWEEN

THE DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS

AND

ST. JOSEPH HEALTH

I. Preamble

St. Joseph Health ("SJH") hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS" or "OCR"). Contemporaneously with this CAP, SJH is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. SJH enters into this CAP as part of the consideration for the release in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

SJH has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Annette M. Walker
Chief Executive-SJH
3345 Michelson Drive, Suite 100
Irvine, California 92612

HHS has identified the following individual as its contact person to whom SJH is to report information regarding implementation of this CAP:

Ms. Emma Roberts, Equal Opportunity Specialist
Department of Health and Human Services
Office for Civil Rights
90 7th Street, Suite 4-100
San Francisco, California 94103-6705

SJH and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions

Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date for this CAP shall be calculated in accordance with paragraph II.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by SJH under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the date HHS approves the last of the policies and procedures, risk analysis, and risk management plan required under section V of this CAP, unless HHS has notified SJH under section VIII hereof of its determination that SJH has breached this CAP. In the event of such a notification by HHS under section VIII hereof, the Compliance Term shall not end until HHS notifies SJH that it has determined that the breach has been cured or HHS proceeds with the imposition of a civil monetary penalty ("CMP") against SJH pursuant to 45 C.F.R. Part 160 and Section VIII.D. of this CAP. After the Compliance Term ends, SJH shall still be obligated to submit the final Annual Report as required by section VI and comply with the document retention requirement in section VII of this CAP.

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. The day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day that is not one of the aforementioned days.

V. Corrective Action Obligations

SJH agrees to the following:

A. Conduct an Enterprise-wide Risk Analysis

1. Within two hundred forty (240) calendar days of the Effective Date, SJH shall provide HHS an accurate and thorough enterprise-wide risk analysis of security risks and vulnerabilities that incorporates all electronic equipment, data systems, and applications controlled, administered, or owned by SJH, its workforce members, and affiliated staff that contains, stores, transmits, or receives electronic protected health information (ePHI) for review. SJH shall develop a complete inventory of all electronic equipment, data systems, and applications that contain or store ePHI, which will be incorporated in its risk analysis. Within sixty (60) days of its receipt of SJH's risk analysis, HHS shall provide the SJH Contact Person with any applicable comments and recommendation for SJH to prepare a revised risk analysis. SJH shall have sixty (60) days in which to revise its risk

analysis accordingly, and then have the SJH Contact Person submit the revised risk analysis to HHS for review and approval. This submission and review process shall continue until HHS approves the risk analysis.

B. Develop and Implement a Risk Management Plan

1. Within sixty (60) calendar days of HHS' approval of the risk analysis required by section V.A.1 of this CAP, SJH shall provide HHS an organization-wide risk management plan to address and mitigate any security risks and vulnerabilities identified in the risk analysis. Within sixty (60) days of its receipt of SJH's risk management plan, HHS will inform the SJH Contact Person of any applicable comments and recommendations for SJH to prepare a revised risk management plan. SJH shall have sixty (60) days in which to revise its risk management plan accordingly, and, through the SJH Contact Person, submit the revised risk management plan to HHS for review and approval. This submission and review process shall continue until HHS approves the risk management plan.
2. Within thirty (30) calendar days of HHS' approval of the risk management plan required by section V.B.1 of this CAP, SJH shall finalize and officially adopt the risk management plan in accordance with its applicable administrative procedures. SJH shall immediately thereafter begin implementation of the risk management plan and shall distribute the plan to workforce members involved with implementation of the plan.

C. Policies and Procedures

1. SJH shall provide HHS with its revised policies and procedures with respect to compliance with 45 C.F.R. 164.502(a). SJH shall provide the policies and procedures to HHS for review and approval within sixty (60) days of HHS' approval of the risk management plan required by section V.B.2 of this CAP. Within sixty (60) days of its receipt of SJH's revised policies and procedures, HHS will inform the SJH Contact Person of any applicable comments and recommendations for SJH to prepare acceptable, revised policies and procedures. Upon receiving any recommended changes to such policies and procedures from HHS, SJH shall have thirty (30) calendar days in which to revise the policies and procedures accordingly, and then submit the revised policies and procedures to HHS for review and approval. This process shall continue until HHS approves the policies and procedures.
2. Within thirty (30) calendar days of HHS final approval of the policies and procedures required by section V.C.1 of this CAP, SJH shall finalize and officially adopt the policies and procedures.

D. Training On Updated Policies and Procedures

1. Within thirty (30) days of HHS' final approval of the policies and procedures required by section V.C.1 of this CAP, SJH shall forward its proposed training materials on the policies and procedures to HHS for its review and approval. Within thirty (30) days of its receipt of SJH's proposed training materials on the policies and procedures, HHS will inform the SJH Contact Person of any applicable comments and recommendations for SJH to prepare acceptable, revised training materials.
2. Within sixty (60) days of HHS' final approval of the training materials, SJH shall provide training to all appropriate workforce members, in accordance with SJH's applicable administrative procedures for training.
3. After providing the training required by section V.D.2 of this CAP, SJH shall provide annual retraining on the training materials OCR approved under this CAP to all appropriate workforce members for the duration of the Compliance Term of this CAP.
4. Each workforce member who is required to receive training shall certify, in electronic or written form, that he or she received the training. The training certification shall specify the date on which the training was received. All training materials shall be retained in compliance with section VII of this CAP.

VI. Reportable Events, Implementation Report, and Annual Report

A. Reportable Events

1. During the Compliance Term, SJH shall, upon receiving information that a workforce member may have failed to comply with any provision of the policies and procedures required by section V.C.1 or section V.D.1 of this CAP, promptly investigate the matter. If SJH determines that a workforce member has materially violated the policies and procedures required by section V.C.1 or section V.D.1 of this CAP, SJH shall notify HHS in writing within sixty (60) days. Such violations shall be known as "Reportable Events." The report to HHS shall include the following:
 - a. A complete description of the event, including relevant facts, the persons involved, and the implicated provision(s) of SJH's policies and procedures; and
 - b. A description of actions taken and any further steps SJH plans to take to address the matter, to mitigate the harm, and to prevent it from recurring, including the application of appropriate sanctions against workforce members who failed to comply with its policies and procedures.

2. If no Reportable Events occur during any one Reporting Period, as defined in section VI.B.1 of this CAP, SJH shall so inform HHS in its Annual Report for that Reporting Period.

B. Annual Reports

1. The one-year period after HHS' last approval of the policies and procedures, risk analysis, and risk management plan required under section V of this CAP, and each subsequent one-year period during the Compliance Term, as defined in section III of this CAP, shall each be known as a "Reporting Period." SJH shall submit to HHS a report with respect to the status of and findings regarding SJH's compliance with this CAP for each Reporting Period ("Annual Report"). SJH shall submit each Annual Report to HHS no later than twenty (20) days after the end of each corresponding Reporting Period. Each Annual Report shall include:
 - a. An attestation signed by an officer of SJH attesting that the policies and procedures and risk management plan required by Section V of this CAP: (a) have been adopted; (b) are being implemented; and (c) have been distributed to all appropriate workforce members;
 - b. A copy of all training materials used for the training required by Section V of this CAP, a description of the training, including a summary of the topics covered, the length of the training session(s) conducted and a schedule of when the training session(s) were held;
 - c. A summary of Reportable Events (defined in section VI.A.1 of this CAP) identified during the Reporting Period and the status of any corrective or preventative action(s) taken by SJH relating to each Reportable Event;
 - d. An attestation signed by an officer of SJH attesting that it has obtained and is maintaining written or electronic certifications from all workforce members that are required to receive training that they received the requisite training pursuant to the requirements set forth on this CAP;
 - e. An attestation signed by an officer of SJH listing all of SJH's locations, the name under which each location is doing business, the corresponding mailing address, phone number and fax number for each location, and attesting that each location has complied with the obligations of this CAP; and
 - f. An attestation signed by an officer of SJH stating that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content, and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

SJH shall maintain for inspection and copying, and shall provide to HHS upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date. Nothing in this agreement shall be construed to constitute a waiver by SJH of any applicable legal privilege against disclosure, including the attorney-client privilege and the work product doctrine. If HHS requests access to information or documentation which SJH seeks to withhold on the basis of an applicable legal privilege against disclosure, including the attorney-client privilege or the attorney work product doctrine, SJH shall provide HHS with a description of such information and the type of privilege asserted.

VIII. Requests for Extensions and Breach Provisions

SJH is expected to fully and timely comply with all provisions contained in this CAP.

A. **Timely Written Requests for Extensions.** SJH may, in advance of any due date in this CAP, submit a timely written request for an extension of time to perform any act or file any notification or report required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least five (5) business days prior to the date by which any act is due to be performed.

B. **Notice of Breach and Intent to Impose CMP.** The Parties agree that a breach of this CAP by SJH constitutes a breach of the Agreement. Upon a determination by HHS that SJH has breached this CAP, HHS may notify SJH of: (1) SJH's breach and (2) HHS' intent to impose a civil monetary penalty (CMP), pursuant to 45 C.F.R. Part 160, for the Covered Conduct in paragraph I.2 of the Agreement and for any other conduct that constitutes a violation of the HIPAA Rules ("Notice of Breach and Intent to Impose CMP").

C. **SJH's Response.** SJH shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. SJH is in compliance with the obligations of this CAP that HHS cited as the basis for the breach;
2. The alleged breach has been cured; or
3. The alleged breach cannot be cured within the 30-day period, but that: (a) SJH has begun to take action to cure the breach; (b) SJH is pursuing such action with due diligence; and (c) SJH has provided to HHS a reasonable timetable for curing the breach.

D. **Imposition of CMP.** If at the conclusion of the 30-day period, SJH fails to meet the requirements of section VIII.C of this CAP to HHS' satisfaction, HHS may proceed with the imposition of the CMP against SJH pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to the Covered Conduct in paragraph I.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify SJH in writing of its determination to proceed with the imposition of a CMP.

For St. Joseph Health

Annette M. Walker
Annette M. Walker
Chief Executive-SJH

10-13-16
Date

For the United States Department of Health and Human Services

Michael Leoz
Michael Leoz
Regional Manager
Office for Civil Rights, Pacific Region

10-13-16
Date

Appendix B

HOSPITAL	LOCATION
Covenant Health System <ul style="list-style-type: none">• Covenant Medical Center• Covenant Medical Center - Lakeside• Covenant Children's Hospital• Covenant Hospital, Levelland• Covenant Hospital, Plainview	Lubbock, TX Roswell, NM
Mission Hospital <ul style="list-style-type: none">• Mission Hospital, Laguna Beach	Mission Viejo, CA Laguna Beach, CA
Petaluma Valley Hospital	Petaluma, CA
Queen of the Valley Medical Center	Napa, CA
Redwood Memorial Hospital	Fortuna, CA
Santa Rosa Memorial Hospital	Santa Rosa, CA
St. Joseph Hospital, Eureka	Eureka, CA
St. Joseph Hospital, Orange	Orange, CA
St. Jude Medical Center	Fullerton, CA
St. Mary Medical Center	Apple Valley, CA