

## 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. Luke's-Roosevelt Hospital Center Inc. ("St. Luke's") is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. St. Luke's, located in New York City, is part of the Mount Sinai Health System (MSHS). HHS and St. Luke's shall together be referred to herein as the "Parties."

### 2. Factual Background and Covered Conduct.

On September 12, 2014, OCR received a complaint against St. Luke's Spencer Cox Center for Health alleging that on September 10, 2014, a staff member impermissibly disclosed the complainant's protected health information (PHI) by faxing his medical records to his employer. On March 11, 2015, HHS notified St. Luke's that it was initiating an investigation regarding St. Luke's compliance with the HIPAA Rules. OCR's investigation indicated that the following conduct occurred ("Covered Conduct"):

- a. St. Luke's impermissibly disclosed PHI of two identified patients when Spencer Cox staff members faxed one individual's PHI to his workplace and the other individual's PHI to an office at which he volunteered. *See* Uses and Disclosures- 45 C.F.R. § 164.502(a). Given the type of PHI involved, specifically information about HIV, AIDS, and mental health, the impermissible disclosures were egregious.
- b. St. Luke's failed to reasonably safeguard two identified patients' PHI from any intentional or unintentional disclosure during faxing, resulting in an impermissible disclosure of both patients' PHI against their expressed instructions. *See* Safeguards - 45 C.F.R. § 164.530(c)(2)(i).

3. No Admission. This Agreement is not an admission of liability by St. Luke's.

4. No Concession. This Agreement is not a concession by HHS that St. Luke's is not in violation of the HIPAA Rules and not liable for civil money penalties ("CMPs").

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number: 14-194017 and any 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 formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

## **II. Terms and Conditions**

6. Payment. HHS has agreed to accept, and St. Luke's has agreed to pay HHS, the amount of \$ 387,200.00 ("Resolution Amount"). St. Luke's 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. St. Luke's 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 St. Luke's breaches the CAP, and fails to cure the breach as set forth in the CAP, then St. Luke's 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 St. Luke's performance of its obligations under this Agreement, HHS releases St. Luke's from any actions it may have against St. Luke's 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 St. Luke's 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 Parties. St. Luke's 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. St. Luke's waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a- 7a) and 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 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 St. Luke's 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.

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 shall be set forth in writing and signed by all Parties.

14. Execution of Agreement and Effective Date. The Agreement shall become effective (*i.e.*, final and binding) upon 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 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, St. Luke's agrees that the time between the Effective Date of this Agreement (as set forth in Paragraph 14) and the date the Agreement may be terminated by reason of St. Luke's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. St. Luke's 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, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5.

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 St. Luke's represent and warrant that they are authorized by St. Luke's 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. Luke's Roosevelt Hospital Center, Inc.**

  
\_\_\_\_\_  
Arthur A. Gianelli  
President, Mount Sinai St. Luke's Hospital

5/4/17  
Date

**For the United States Department of Health and Human Services**

  
\_\_\_\_\_  
Linda C. Colón  
Regional Manager  
Eastern and Caribbean Region  
Office for Civil Rights

5/8/17  
Date

Appendix A

**CORRECTIVE ACTION PLAN**

**BETWEEN THE**

**DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**AND**

**ST. LUKE'S-ROOSEVELT HOSPITAL CENTER INC.**

**I. Preamble**

St. Luke's-Roosevelt Hospital Center, Inc. (hereinafter known as "St. Luke's") hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS"). Contemporaneously with this CAP, St. Luke's is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. St. Luke's enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement.

**II. Contact Persons and Submissions**

**A. Contact Persons**

St. Luke's 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:

Louis Schenkel, Esq.  
Vice President and Chief Privacy Officer  
Mount Sinai Health System  
150 East 42<sup>nd</sup> Street, 3<sup>rd</sup> Floor  
New York, New York 10017  
[Louis.Schenkel@mountsinai.org](mailto:Louis.Schenkel@mountsinai.org)

HHS has identified the following individual as its authorized representative and contact person with whom St. Luke's is to report information regarding the implementation of this CAP:

Linda C. Colón, Regional Manager  
Eastern and Caribbean Region  
Office for Civil Rights  
U.S. Department of Health and Human Services  
26 Federal Plaza, Suite 3312  
New York, New York 10278  
Voice Phone (212) 264-4136  
Fax: (212) 264-4136

St. Luke's 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, electronic mail ("email") 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 St. Luke's under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the Effective Date, unless HHS has notified St. Luke's under Section VIII hereof of its determination that St. Luke's breached this CAP. In the event HHS notifies St. Luke's of a breach under section VIII hereof, the Compliance Term shall not end until HHS notifies St. Luke's that HHS has determined St. Luke's failed to meet the requirements of section VIII.C of this CAP and issues a written notice of intent to proceed with an imposition of a civil money penalty against St. Luke's pursuant to 45 C.F.R. Part 160. After the Compliance Term ends, St. Luke's shall still be obligated to: (a) submit the final Annual Report as required by section VI; and (b) comply with the document retention requirement in section VII. Nothing in this CAP is intended to eliminate or modify St. Luke's obligation to comply with the document retention requirements in 45 C.F.R. § 164.316(b) and § 164.530(j).

### 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 which is not one of the aforementioned days.

### V. Corrective Action Obligations

St. Luke's agrees to the following:

#### A. Policies and Procedures

1. St. Luke's shall review and revise, as necessary, its written policies and procedures concerning the uses and disclosures of protected health information (45 C.F.R. Parts 160 and 164, Subparts A and E, the Privacy Rule), which may include by mail, fax, or other electronic transmission, to comply with the Federal standards that govern the privacy and security of individually identifiable health information.

2. St. Luke's shall provide such policies and procedures consistent with paragraph 1 above, to HHS within thirty (30) calendar days of the Effective Date for review and approval. HHS shall provide any comments on or approve the policies and procedures within sixty (60) calendar days of receipt. Upon receiving any recommended changes to such policies and procedures from HHS, St. Luke's shall have thirty (30) days to revise such policies and procedure accordingly and provide the revised policies and procedures to HHS for review and approval. HHS shall provide any further comments on or approve the revised policies and procedures within thirty (30) calendar days of receipt. This process shall continue until HHS approves the policies and procedures.

#### B. Distribution and Updating of Policies and Procedures

1. St. Luke's shall distribute the policies and procedures identified in section V.A. to all members of the workforce within thirty (30) days of HHS approval of such policies and to new members of the workforce within thirty (30) days of their beginning of service.

2. St. Luke's shall require, at the time of distribution of such policies and procedures, a signed written or electronic initial compliance certification from all members of the workforce stating that the workforce members have read, understand, and shall abide by such policies and procedures.

3. St. Luke's shall assess, update, and revise as necessary, the policies and procedures as appropriate at least annually (and more frequently if appropriate).

#### C. Training

1. St. Luke's shall review and revise, as necessary, its current training materials to include instructions on safeguarding PHI when providing individuals such information, which shall include instructions on providing individuals with such information by mail, fax, or other electronic transmission. St. Luke's shall provide HHS with the training materials for all workforce members within thirty (30) calendar days of the Effective Date. HHS shall provide any comments on or approve the training materials within sixty (60) calendar days of receipt.

2. Upon receiving notice from HHS specifying any required changes, St. Luke's shall make the required changes and provide revised training materials to HHS within thirty (30) calendar days. HHS shall provide any further comments on or approve the revised materials within thirty (30) calendar days of receipt. This process shall continue until HHS approves the training materials.

3. Upon receiving approval from HHS, St. Luke's shall provide training using the approved training materials for all workforce members within the later of sixty (60) calendar days of HHS' approval or by October 31, 2017. St. Luke's shall also provide training using the approved training materials at least every twelve (12) months thereafter. St. Luke's shall also provide such training to each workforce member that is responsible for faxing and transmitting PHI within thirty (30) calendar days of the commencement of such workforce member's service.

4. Each workforce member who is required to attend training shall certify, in electronic or written form, that he or she has received the training. The training certification shall specify the date training was received. All course materials shall be retained in compliance with Section VII.

5. St. Luke's shall review the training at least annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during audits or reviews, and any other relevant developments.

6. St. Luke's shall not provide access to PHI to any member of its workforce if that workforce member has not signed or provided the written or electronic certification required by Paragraph V.B.2 of this section within three (3) months of distribution of such policies and procedures to the members of its workforce, but in any event no later than January 31, 2018.

#### D. Reportable Events

During the Compliance Term, St. Luke's shall, upon learning that a workforce member may have failed to comply with the policies and procedures required by section V.A.1 of this CAP, promptly investigate the matter. If St. Luke's determines, after review and investigation, that a member of its workforce has failed to comply with these policies and procedures, St. Luke's shall notify in writing HHS within thirty (30) calendar days of reaching such determination. Such violations shall be known as "Reportable Events." If the assets of St. Luke's are merged with the assets of one or more other covered entities, after such merger this Section V.D. of the CAP will continue to apply, but only to any of the facilities, offices, programs, or operations that were part of St. Luke's as of the Effective Date, as identified in Appendix B. The report to HHS shall include the following information:

1. A complete description of the event, including the relevant facts, the persons involved, and the applicable provision(s) of St. Luke's Privacy, Security, and Breach Notification policies and procedures; and

2. A description of the actions taken and any further steps St. Luke's plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including application of any appropriate sanctions against workforce members who failed to comply with its Privacy, Security, and Breach Notification policies and procedures.

### VI. Implementation Report and Annual Reports

A. Implementation Report. Within ninety (90) days after HHS approves the policies and procedures specified in Section V.B.1 above, St. Luke's shall submit a written report with the documentation described below to HHS for review and approval ("Implementation Report"). The Implementation Report shall include:

1. An attestation signed by an owner or officer of St. Luke's attesting that the policies and procedures are being implemented, have been distributed to all appropriate members of the workforce, and that St. Luke's has obtained all of the compliance certifications required by Sections V.B.2;

2. A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held;

3. An attestation signed by an owner or officer of St. Luke's attesting that all members of the workforce have completed the initial training required by this CAP and have executed the training certifications required by Section V.C.4;

4. An attestation signed by an owner or officer of St. Luke's listing all St. Luke's locations (including locations and mailing addresses), the corresponding name under which each location is doing business, the corresponding phone numbers and fax numbers, and attesting that each such location has complied with the obligations of this CAP; and

5. An attestation signed by an owner or officer of St. Luke's stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

B. Annual Reports. The one-year period beginning on the Effective Date and each subsequent one-year period during the course of the period of compliance obligations shall be referred to as "the Reporting Periods." St. Luke's also shall submit to HHS Annual Reports with respect to the status of and findings regarding St. Luke's compliance with this CAP for each of the three (3) year Reporting Periods. St. Luke's shall submit each Annual Report to HHS no later than sixty (60) calendar days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A schedule, topic outline, and copies of the training materials for the training programs attended in accordance with this CAP during the Reporting Period that is the subject of the report;

2. An attestation signed by an owner or officer of St. Luke's attesting that it is obtaining and maintaining written training certifications from all persons that require training that they received training pursuant to the requirements set forth in this CAP;

3. A summary of Reportable Events (defined in Section V.D) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

4. An attestation signed by an owner or officer of St. Luke's attesting 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**

St. Luke's 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.

## **VIII. Breach Provisions**

St. Luke's is expected to fully and timely comply with all provisions contained in this CAP.

### **A. Timely Written Requests for Extensions**

St. Luke's may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least five (5) days prior to the date such an act is required or due to be performed. The requirement may be waived by OCR only.

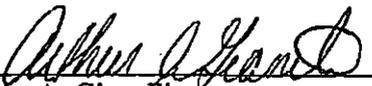
**B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty.** The parties agree that a breach of this CAP by St. Luke's constitutes a breach of the Agreement. Upon a determination by HHS that St. Luke's has breached this CAP, HHS may notify St. Luke's of: (1) St. Luke's breach; and (2) HHS' intent to impose a CMP pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct set forth in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Privacy, Security, or Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

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

1. St. Luke's is in compliance with the obligations of the 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 thirty (30) calendar day period, but that: (a) St. Luke's has begun to take action to cure the breach; (b) St. Luke's is pursuing such action with due diligence; and (c) St. Luke's has provided to HHS a reasonable timetable for curing the breach.

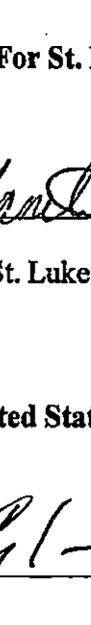
**D. Imposition of CMP.** If at the conclusion of the thirty (30) day calendar period, St. Luke's fails to meet the requirements of Section VIII.C. of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against St. Luke's pursuant to 45 C.F.R. Part 160 for any violations of the Covered Conduct set forth 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 St. Luke's in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

**For St. Luke's-Roosevelt Hospital Center, Inc.**

  
\_\_\_\_\_  
Arthur A. Gianelli  
President, Mount Sinai St. Luke's Hospital

  
\_\_\_\_\_  
Date

**For United States Department of Health and Human Services**

  
\_\_\_\_\_  
Linda C. Colón  
Regional Manager  
Eastern and Caribbean Region  
Office for Civil Rights

  
\_\_\_\_\_  
Date

**APPENDIX B**

Mount Sinai St. Luke's  
1111 Amsterdam Avenue  
New York, New York 10025

Mount Sinai West (formerly Roosevelt Hospital)  
1000 Tenth Avenue  
New York, New York 10019

Samuels Clinic (formerly Spencer Cox Clinic)  
1000 Tenth Avenue, Suite 2T  
New York, New York 10019

Ambulatory Psychiatric Center  
411 West 114<sup>th</sup> Street  
New York, New York 10025

Morningside Clinic (formerly Spencer Cox Clinic)  
440 West 114<sup>th</sup> Street  
Clark Building, 6<sup>th</sup> Floor  
New York, NY 10025

SLR Community Care Center at 59<sup>th</sup> Street  
425 West 59th Street  
New York, New York 10019