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 ("PHI") (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. Elizabeth's Medical Center ("SEMC"), which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. SEMC is a tertiary care hospital located in Brighton, Massachusetts that offers both inpatient and outpatient services.

HHS and SEMC shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct

On November 16, 2012, HHS received a complaint alleging noncompliance with the HIPAA Rules by SEMC workforce members, including the use of an internet-based document sharing application to store documents containing electronic protected health information ("ePHI") of at least 498 individuals. On February 14, 2013, HHS notified SEMC of its investigation into the allegations and SEMC's compliance with the HIPAA Rules (HHS Transaction Number 13-151444). Then, on August 25, 2014, SEMC submitted notification to HHS pursuant to the requirement under 45 C.F.R. § 164.408 regarding a breach of unsecured ePHI stored on a former SEMC workforce member's personal laptop and USB flash drive, affecting 595 individuals. On November 17, 2014, HHS notified SEMC of HHS' investigation regarding SEMC's compliance with the HIPAA Rules (HHS Transaction Number 14-190416).

HHS' investigations indicated that the following conduct occurred, which shall be defined as "Covered Conduct" for the purposes of this Agreement:

(1) SEMC disclosed the PHI of at least 1,093 individuals. (*See* 45 C.F.R. §§ 160.103 and 164.502 (a).)

(2) SEMC failed to implement sufficient security measures regarding the transmission of and storage of ePHI to reduce risks and vulnerabilities to a reasonable and appropriate level. (*See* 45 C.F.R. §164.308(a)(1)(ii)(B).)

(3) SEMC failed to timely identify and respond to a known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome. (*See* 45 C.F.R. § 164.308(a)(6)(ii).)

3. No Admission. This Agreement is not an admission, concession, or evidence of liability by SEMC 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 SEMC'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 SEMC is not in violation of the HIPAA Rules and that SEMC is not liable for civil money penalties ("CMPs").

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Numbers 13-151444 and 14-190416, 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. HHS has agreed to accept, and SEMC has agreed to pay HHS, the amount of $218,400 ("Resolution Amount"). SEMC 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. SEMC 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 SEMC breaches the CAP, and fails to cure the breach as set forth in the CAP, then SEMC will be in breach of this Agreement, and HHS will not be subject to the terms and conditions in the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon SEMC's performance of its obligations under this Agreement, HHS releases SEMC and its successors, transferees, assigns, parents, subsidiaries, members, agents, directors, officers, affiliates and employees from any claims, actions, or causes of action it 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 SEMC 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. SEMC 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. SEMC 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 SEMC 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 shall be set forth in writing and signed by both Parties. Nothing in this Agreement is intended to, or shall, be used as any basis for the denial of any license, authorization, approval, or consent that SEMC may require under any law, rule, or regulation.

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 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, SEMC agrees that the time between the Effective Date of this Agreement and the date this Agreement may be terminated by reason of SEMC'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. SEMC 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 of this Agreement 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; provided, however, that HHS will use its best efforts to prevent the disclosure of information, documents, and any other item produced by SEMC to HHS as part of HHS' 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 signing this Agreement on behalf of SEMC represents and warrants that he is authorized to execute this Agreement. The individual signing this Agreement on behalf of HHS represents and warrants that she is signing this Agreement in her official capacity and that she is authorized to execute this Agreement.

For St. Elizabeth's Medical Center

-//- July 8, 2015

Roger Mitty, M.D. Date
Interim President

For the United States Department of Health and Human Services

-//- July 8, 2015

Susan M. Pezzullo Rhodes Date
Regional Manager, Region I
Office for Civil Rights

Appendix A CORRECTIVE

ACTION PLAN BETWEEN

THE

DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

ST. ELIZABETH'S MEDICAL CENTER

I. Preamble

St. Elizabeth's Medical Center ("SEMC"), 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, SEMC is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. SEMC enters into this CAP as part of the consideration for the release set forth in Section II.8. of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

SEMC 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:

Michael F. Collins
Chief Administrative Officer
St. Elizabeth's Medical Center
735 Cambridge Street
Brighton, MA 02135
Michael.Collins@steward.org
Telephone: 617-789-2366
Facsimile: 617-562-7568

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

Ms. Susan M. Pezzullo Rhodes, Regional Manager
Office for Civil Rights, Region I
Department of Health and Human Services
JFK Federal Building, Room 1875
Boston, MA 02203
Susan.Rhodes@hhs.gov

Telephone: 617-565-1347
Facsimile: 617-565-3809

SEMC 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, 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 SEMC under this CAP shall begin on the Effective Date of this CAP and end one (1) year from the Effective Date unless HHS has notified SEMC under Section VIII. hereof of its determination that SEMC 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 SEMC that it has determined that the breach has been cured or HHS proceeds with the imposition of a civil monetary penalty ("CMP") against SEMC pursuant to 45 C.F.R. Part 160 and Section VIII.D. of the CAP. After the Compliance Term ends, SEMC shall still be obligated to submit the Implementation Report as required by Section VI. of the CAP and to comply with the document retention requirement in Section VII. of the 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 which is not one of the aforementioned days.

V. Corrective Action Obligations

SEMC agrees to the following:

A. SEMC Self-Assessment

1. Purpose of Self-Assessment: Within one hundred twenty (120) calendar days of the Effective Date, SEMC or its designee shall conduct an assessment in accordance with Section V.A.2. of SEMC workforce members' familiarity and compliance with SEMC policies and procedures that address the following:

a. transmitting ePHI using unauthorized networks;

b. storing ePHI on unauthorized information systems, including unsecured networks and devices;

c. removal of ePHI from SEMC;

d. prohibition on sharing accounts and passwords for ePHI access or storage;

e. encryption of portable devices that access or store ePHI; and

f. security incident reporting related to ePHI.

2. Description of Self-Assessment: Self-Assessment will include, but not be limited to:

a. Unannounced site visits to five SEMC departments, including the Cardiology Department (the "Covered Departments") to assess implementation of the policies and procedures described in Section V.A.1.;

b. Interviews with a total of fifteen (15) randomly selected SEMC workforce members who have access to ePHI, thirteen (13) of whom shall be from the Covered Departments— including at least one intern, resident, or fellow, and the remaining two (2) of whom shall be interns, residents, or fellows working in Hematology/Oncology; and

c. Inspection of at least three (3) portable devices at each of the Covered Departments that can access ePHI, including one (1) laptop, one (1) other portable device, such as a tablet or smartphone, and one (1) portable storage media, such as a USB flash drive, randomly selected to ensure that such devices satisfy all applicable requirements of the policies and procedures described in Section V.A.1.

3. Self-Assessment Report: Within one hundred fifty (150) calendar days of the Effective Date, SEMC or its designee shall prepare a written report documenting the Self-Assessment, and provide such report to HHS (Self-Assessment Report). The Self-Assessment Report shall include, but not be limited to:

a. Dates and locations of unannounced site visits;

b. Job titles and duties of workforce members interviewed;

c. Summaries of results of interviews;

d. Summaries of inspections of workstations and other devices containing ePHI; and

e. Identification of any material compliance issues with the policies described in Section V.A.1., and recommendations for improving these policies and procedures, oversight and supervision, or training.

B. Policies and Procedures

1. If SEMC determines that the policies and procedures shall be revised pursuant to Section V.A.3.e., SEMC shall draft the appropriate revisions for review by HHS. If the Self-Assessment indicates that SEMC workforce members are unfamiliar with or not substantially complying with SEMC's policies and procedures described in Section V.A.1., and SEMC concurs, SEMC shall develop an oversight mechanism reasonably tailored to ensure that all SEMC workforce members follow such policies and procedures, and that ePHI is only used and disclosed as provided for by such policies and procedures.

2. SEMC shall provide any policies and procedures or any oversight mechanism that may be revised as provided in Section V.B.1., to HHS for its review within thirty (30) calendar days of providing HHS with the Self-Assessment Report. HHS will review any revised policies and procedures to ensure they are consistent with the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule") and the Federal Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule").

3. Upon receiving HHS' notice of recommended revisions, if any, SEMC shall have thirty (30) calendar days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review.

4. Within thirty (30) calendar days after receiving HHS' final approval of any revisions to the policies and procedures described in Section V.B.1., SEMC shall implement and distribute the policies and procedures to all appropriate workforce members.

C. Training

1. If SEMC determines that the training shall be revised pursuant to Section V.A.3.e., SEMC shall draft the appropriate revisions for review by HHS. HHS will review any revised training materials to ensure they are consistent with the Federal Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule") and the Federal Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule").

2. SEMC shall provide any draft training that may be revised as provided in Section V.C.1, to HHS within sixty (60) calendar days of providing HHS with the Self-Assessment Report.

3. Upon receiving HHS' notice of recommended revisions, if any, SEMC shall have thirty (30) calendar days to revise the workforce training and provide the revised training to HHS for review.

4. Within thirty (30) calendar days after receiving HHS' final approval of the revised workforce training described in Section V.C.1., SEMC shall distribute a security reminder reflecting the content of such training and describing any revised policies and procedures to all SEMC workforce members who have access to ePHI. SEMC shall incorporate the revised training into its next annual refresher training for all applicable SEMC workforce members. SEMC shall provide such training to new members of the workforce who have access to ePHI within sixty (60) calendar days of the workforce members beginning their service.

5. Each individual who is required to attend training shall certify, in writing or in electronic form, that the individual has received the required training. The training certification shall specify the date training was completed. A sign-in sheet shall suffice to meet this requirement. All course materials shall be retained in compliance with Section VII.

D. Reportable Events.

1. Beginning one hundred eighty (180) calendar days after the Effective Date, SEMC shall, upon receiving information that a workforce member may have failed to comply with its policies and procedures described in Section V.A.1., promptly investigate this matter. If SEMC determines, after review and investigation, that a member of its workforce has failed to comply with these policies and procedures, SEMC shall report such events to HHS as provided in Section VI.1.d. Such violations shall be known as "Reportable Events." The report to HHS shall include the following information:

a. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures implicated, except that, for non-material violations of policies and procedures investigated pursuant to receipt of notification generated by its data loss prevention software, SEMC may report multiple, similar incidents in the aggregate without reference to the individual persons involved. Aggregate reporting shall only apply to an individual's first non-material violation; and

b. A description of the actions taken and any further steps SEMC plans to take or takes 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 policies and procedures.

c. If no reportable events occur within the Compliance term, SEMC shall so inform HHS as provided in Section VI.1.d.

VI. Implementation Report

1. Within one (1) year after the Effective Date, SEMC shall submit a written report to HHS for its review and approval ("Implementation Report"). The Implementation Report shall include:

a. An attestation signed by an officer of SEMC attesting that any new policies and procedures developed under Section V.B have been implemented and distributed to all appropriate members of the workforce consistent with the requirements in Section V.B.;

b. a summary of the length and content of any training session(s) required by this CAP and a schedule of when the training session(s) were held;

c. An attestation signed by an officer of SEMC attesting that all members of the workforce identified in Section V.C.4. have completed any new training required by this CAP and have executed the training certifications required by Section V.C.5.;

d. A summary of Reportable Events identified beginning one hundred eighty (180) calendar days of the Effective Date as defined in section V.D.1.;

e. An attestation signed by an officer of SEMC 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.

VII. Document Retention

SEMC 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 SEMC of any applicable legal privilege against disclosure, including the attorney-client privilege and the work product doctrine. If OCR requests access to information or documentation which SEMC seeks to withhold on the basis of an applicable legal privilege against disclosure, including the attorney-client privilege or the attorney work product doctrine, SEMC shall provide OCR with a description of such information and the type of privilege asserted.

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions. SEMC 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) calendar days prior to the date such an act is required or due to be performed.

B. Notice of Breach of this CAP and Intent to Impose CMP. The Parties agree that a breach of this CAP by SEMC that has not been cured in accordance with Section VIII.C., below, constitutes a breach of the Agreement. Upon a determination by HHS that SEMC has breached this CAP, HHS may notify SEMC of (1) SEMC's breach; and (2) HHS' intent to impose a CMP, pursuant to 45 C.F.R. Part 160, for the Covered Conduct in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Rules ("Notice of Breach and Intent to Impose CMP").

C. SEMC Response. SEMC 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. SEMC 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) SEMC has begun to take action to cure the breach; (b) SEMC is pursuing such action with due diligence; and (c) SEMC has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, SEMC fails to meet the requirements of Section VIII.C. to HHS' satisfaction, HHS may proceed with the imposition of the CMP against SEMC pursuant to the rights and obligations set forth in 45 C.F.R. Part 160 for any violations of the HIPAA Rules for 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 inform SEMC in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. §§ 160.312(a)(3)(i) and (ii).

For St. Elizabeth's Medical Center

-//- July 8, 2015

Roger Mitty, M.D. Date
Interim President

For the United States Department of Health and Human Services

-//- July 8, 2015

Susan M. Pezzullo Rhodes Date
Regional Manager, Region I
Office for Civil Rights