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. Lahey Clinic Hospital, Inc. ("Lahey"), which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. Lahey is a nonprofit teaching hospital. It has over 500 physicians and 5,000 nurses, therapists, and other support staff, treating nearly 719,000 outpatients and 18,000 inpatients last year.[1]

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

2. Factual Background and Covered Conduct

On October 11, 2011, HHS received notification from Lahey regarding a breach of its unsecured electronic protected health information ("ePHI"). Lahey reported that an unencrypted laptop used in connection with a computerized tomography ("CT") scanner, which contained certain ePHI of approximately 599 individuals, was stolen from an unlocked treatment room off of the inner corridor of Lahey's Radiology Department. By letter dated November 9, 2011, OCR notified Lahey of OCR's investigation regarding Lahey's compliance with the HIPAA Rules. OCR's investigation indicated that the following conduct occurred ("Covered Conduct"):

(1) Lahey failed to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI as part of its security management process. See 45 C.F.R. §164.308(a)(1)(ii)(A).

[1] http://www.lahey.org/About_Lahey.aspx

(2) Lahey failed to implement reasonable and appropriate physical safeguards for a workstation that accesses ePHI to restrict access to authorized users. See 45 C.F.R. § 164.310(c).

(3) With respect to the workstation, Lahey failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility. See 45 C.F.R. § 164.310(d)(1).

(4) Lahey failed to assign a unique user name for identifying and tracking user identity with respect to the aforementioned workstation. See 45 C.F.R. § 164.312(a)(2)(i).

(5) Lahey did not implement a mechanism to record and examine activity on the workstation at issue in this breach. See 45 C.F.R. § 164.312(b).

(6) Lahey impermissibly disclosed the ePHI of 599 individuals for a purpose not permitted by the Privacy Rule. See 45 C.F.R. § 164.502(a).

3. No Admission. This Agreement is not an admission, concession, or evidence of liability by Lahey 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 Lahey'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 Lahey 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 HHS Transaction Number: 01-12-133991, 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 Lahey has agreed to pay HHS, the amount of $850,000.00 ("Resolution Amount"). Lahey 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. Lahey 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 Lahey breaches the CAP, and fails to cure the breach as set forth in the CAP, then Lahey 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 Lahey's performance of its obligations under this Agreement, HHS releases Lahey 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 Lahey 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. Lahey 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. Lahey 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 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 Lahey 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 Lahey 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 (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 the Agreement, Lahey agrees that the time between the Effective Date of this Agreement and the date this Agreement may be terminated by reason of Lahey'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. Lahey 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 Lahey 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 Lahey represents and warrants that (s)he is authorized by Lahey 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 capacities and that she is authorized to execute this Agreement.

For Lahey Clinic Hospital, Inc.

/s/ 11/19/15

David G. Spackman
General Counsel and Senior Vice President, Governmental Affairs
Lahey Clinic Hospital, Inc.

Date

For the United States Department of Health and Human Services

/s/ 11/19/15

Susan Rhodes
Regional Manager, Region I Office for Civil Rights

Date

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

LAHEY CLINIC HOSPITAL, INC.

I. Preamble

Lahey Clinic Hospital, Inc. (Lahey) 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, Lahey is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. Lahey enters into this CAP as part of the consideration for the release set forth in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

Lahey 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:

Deborah Hesford DosSantos
Deputy General Counsel
Lahey Clinic Hospital, Inc.
41 Mall Road
Burlington, MA 01805
Deborah.H.DosSantos@lahey.org
Telephone: 781-744-7544 Facsimile: 781-744-5445

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

Ms. Susan 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

Lahey 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 Lahey under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date unless HHS has notified Lahey under section VIII hereof of its determination that Lahey 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 Lahey that it has determined that the breach has been cured or HHS proceeds with the imposition of a civil monetary penalty ("CMP") against Lahey pursuant to 45 C.F.R. Part 160 and section VIII.D. of the CAP. After the Compliance Term ends, Lahey 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

Lahey agrees to the following:

A. Security Management Process

1. Lahey shall conduct a comprehensive, organization-wide risk analysis of the security risks and vulnerabilities to the ePHI created, received, maintained or transmitted by Lahey that incorporates all of the electronic media, workstations, and information systems owned, controlled or leased by Lahey. The risk analysis shall include all ePHI maintained by Lahey, and include but not be limited to, ePHI stored on and accessed by workstations utilized in connection with diagnostic/laboratory equipment. Security risks and vulnerabilities specific to the ePHI in categories of media, workstations, information systems, may be evaluated as such, provided that there is a reasonable basis on which to believe that such security risks and vulnerabilities are common to the ePHI in each identified category, and the identified and evaluated categories collectively include all of the ePHI created, received, maintained, or transmitted by such media, workstations, and information systems.

2. Within fourteen (14) days of the Effective Date, Lahey shall submit to HHS the methodology by which it proposes to conduct the risk analysis described in paragraph V.A.1. HHS shall notify Lahey whether the proposed methodology is or is not consistent with 45 C.F.R. §164.308(a)(1)(ii)(A).

3. Lahey shall develop a risk management plan to address and mitigate any security risks and vulnerabilities following the risk analysis specified in paragraph V.A.1.

4. The risk analysis report and risk management plan shall be forwarded to HHS for review and approval within two hundred seventy (270) days of the date on which Lahey receives HHS's notification pursuant to section V.A.2. HHS shall approve or, if necessary to ensure compliance with 45 C.F.R. §164.308(a)(1)(ii)(A)–(B), require revisions to Lahey's risk analysis and risk management plan.

5. Upon receiving HHS's notice of required revisions, if any, Lahey shall have ninety (90) days to revise the risk analysis and risk management plan accordingly and forward to HHS for review and approval.

B. <u>Policies and Procedures</u>

1. Within ninety (90) days of HHS's approval of Lahey's risk analysis report and risk management plan, Lahey shall develop or revise, as necessary, written policies and procedures ("Policies and Procedures") to address the Covered Conduct specified in paragraph I.2 of the Agreement to comply with the Federal standards that govern the privacy and security of individually identifiable health information stored, transmitted, or accessed by workstations utilized in connection with diagnostic/laboratory equipment. The Policies and Procedures shall include a procedure or process for:

a. maintaining a record of receipt, removal, and disposition of hardware and electronic media that maintain ePHI into and out of Lahey's facility, and the movement of these items within its facility;

b. ensuring workstations that maintain ePHI utilized in connection with diagnostic/laboratory equipment are registered with Lahey's Information Services Department ("ISD") and under the control of ISD; and

c. implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use workstations that maintain ePHI utilized in connection with diagnostic/laboratory equipment.

2. Within ninety (90) days of HHS's approval of Lahey's risk analysis report and risk management plan, Lahey shall provide the Policies and Procedures, consistent with paragraph V.B.1 above, to HHS for review and approval. HHS shall approve or, if necessary, require revisions to the Policies and Procedures. Such revisions shall be for the purpose of ensuring that Lahey complies with the Security Rule. Upon receiving any required changes to

such Policies and Procedures from HHS, Lahey shall have thirty (30) days to revise the Policies and Procedures accordingly and provide the revised Policies and Procedures to HHS for review and approval.

3. Within thirty (30) days of HHS's final approval, Lahey shall finalize and implement the Policies and Procedures in accordance with its applicable administrative procedures.

C. Training

Within ninety (90) days of HHS's approval of the Policies and Procedures, Lahey shall provide specific training on the Policies and Procedures to all workforce members who access ePHI. Lahey shall provide such training to new workforce members who have access to and use ePHI, within thirty (30) days of beginning service.

D. Reportable Events

1. After the implementation of the Policies and Procedures under section V.B.3., Lahey shall, during the remainder of the Compliance Term, upon receiving information that a workforce member may have failed to comply with any policies and procedures related to the issues referenced in Section V.B.1 above, promptly investigate the matter. If Lahey, after review and investigation, determines that a member of its workforce has failed to comply with such policies and procedures, Lahey shall report such events to HHS as provided in section VI.A.6. Such violations shall be known as "Reportable Events." The report to HHS shall include the following:

a. A complete description of the event, including the relevant facts, the persons involved, and the applicable provision(s) of Lahey's policies and procedures; and

b. A description of actions taken and any further steps Lahey plans to take or takes to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of any appropriate sanctions against workforce members who failed to comply with any applicable policies and procedures.

2. If no Reportable Events occur during the remainder of the Compliance Term, Lahey shall so inform HHS in the Implementation Report as specified in section VI below.

VI. Implementation Report

A. Within one-hundred and eighty (180) days after HHS approves Policies and Procedures specified in section V.B. above, Lahey 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 officer of Lahey attesting that the Policies and Procedures required by section V.B. have been implemented;

2. A description and documentation of how Lahey implemented mechanism(s) to record and examine activity in information systems required by section V.B.;

3. An attestation signed by an officer of Lahey attesting that the mechanism(s) required by section V.B. have been implemented;

4. An explanation of how Lahey implemented its security management process consistent with section V.A. above, focusing specifically on how Lahey determined whether its policies and procedures should be revised based on the risks and vulnerabilities identified in the risk analysis.

5. An attestation signed by an officer of Lahey attesting that any revised policies and procedures have been fully implemented and that all members of the workforce who have access to ePHI have completed training on any revised policies and procedures consistent with the requirements in section V.C.;

6. A summary of Reportable Events, if any, the status of any corrective and preventative action(s) relating to all such Reportable Events, or an attestation signed by an officer of Lahey stating that no Reportable Events occurred during the Compliance Term.

7. An attestation signed by an officer of Lahey 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

Lahey 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 Lahey 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 Lahey seeks to withhold on the basis of an applicable legal privilege against disclosure, including the attorney-client privilege or the attorney work product doctrine, Lahey shall provide HHS with a description of such information and the type of privilege asserted.

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions. Lahey 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 Lahey that has not been cured in accordance with section VIII.C., below, constitutes a breach of the Agreement. Upon a determination by HHS that Lahey has breached this CAP, HHS may notify Lahey of: (1) Lahey's breach; and (2) HHS' intent to impose a CMP, pursuant to 45 C.F.R. Part 160, 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. Lahey Response. Lahey 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. Lahey 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 30-day period, but that: (a) Lahey has begun to take action to cure the breach; (b) Lahey is pursuing such action with due diligence; and (c) Lahey has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, Lahey 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 Lahey 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 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 Lahey 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 Lahey Clinic Hospital, Inc.

/s/ 11/19/15

David G. Spackman
General Counsel and Senior Vice President, Governmental Affairs
Lahey Clinic Hospital, Inc.

Date

For the United States Department of Health and Human Services

/s/ 11/19/15

Susan Rhodes
Regional Manager, Region I Office for Civil Rights

Date