COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss. SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,	)
Plaintiff,	)
v.	)
SOUTH SHORE HOSPITAL, INC.,	)
Defendant.	)

FINAL JUDGMENT BY CONSENT OF DEFENDANT SOUTH SHORE HOSPITAL, INC.

The Court has reviewed the Complaint filed in this case by the Commonwealth of Massachusetts through the Attorney General's Office ("Commonwealth"), the Joint Motion for Entry of Final Judgment by Consent, and the attached Consent. The Court finds that it properly has subject matter jurisdiction of this Complaint and personal jurisdiction over Defendant South Shore Hospital, Inc. ("SSH"), and finds that the entry of this Final Judgment by Consent ("Final Judgment") is in the interests of justice.

WHEREAS, the Attorney General has concluded an investigation into the policies, procedures, and practices of SSH regarding its protection of personal information ("PI") and protected health information ("PHI") of residents of the Commonwealth;

WHEREAS, the Attorney General's investigation pertained to allegations that SSH engaged in unfair or deceptive acts or practices by not properly protecting PI and

PHI stored on unencrypted back-up computer tapes that were shipped off-site for destruction, in violation of state rules and regulations designed to protect personal and health information, including G.L. c. 93A, as well as federal law;

WHEREAS, the HITECH Act § 13410(e) gives State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules, 45 C.F.R. §§ 160 and 164, to obtain damages on behalf of state residents and to enjoin further violations of these Rules, which prohibit the unauthorized disclosure of patients' PHI and establish the federal minimum standards that must be followed to protect such information;

WHEREAS, the Commonwealth filed a Complaint against SSH, which is a covered entity under HIPAA, alleging that SSH violated various standards of the HIPAA Privacy Rule, found at 45 C.F.R. § 164 Subparts A and E;

WHEREAS, SSH does not admit to the validity of any of the allegations in the Complaint or to any wrongdoing, violation of any law, or liability to the Attorney General or any other person or entity;

WHEREAS, without any admission of liability, in order to amicably resolve their differences concerning the Complaint and in order to avoid the cost and uncertainty of litigation, the parties have agreed to entry of this Final Judgment; and

WHEREAS, the parties have filed a joint motion seeking entry of this Final Judgment;

Accordingly, **IT IS HEREBY ORDERED AND ADJUDGED THAT:**

I. DEFINITIONS

1. "Business Associate" or "B.A." shall mean that term as it is defined in 45 C.F.R. § 160.103.
2. "Effective Date" shall mean the date of entry of the Final Judgment.
3. "Evergreen agreement" shall mean agreements between SSH and third-parties that are automatically renewed upon completion of a given term or period of time.
4. "Laws Related to Data Security" shall mean HIPAA, G.L. c. 93H, G.L. c. 93I, and 201 C.M.R. 17.00 *et seq.*
5. "Personal Information" or "PI" shall mean that term as it is defined in G.L. c. 93H and 201 C.M.R. 17.02.
6. "Protected Health Information" or "PHI" shall mean that term as it is defined in 45 C.F.R. § 160.103.
7. "Service Provider" shall mean that term as it is defined in 201 CMR 17.02.
8. "WISP" shall mean a written information security plan, as described in 201 CMR 17.03.

II. PARTIES SUBJECT TO JUDGMENT

9. This Final Judgment shall extend to SSH as well as any predecessors, successors, and assigns, and shall constitute a continuing obligation.

III. INJUNCTIVE RELIEF

10. SSH shall comply with G.L. c. 93H by reporting data breaches to the Commonwealth and to the Office of Consumer Affairs and Business

Regulations and providing proper notice of data breaches to Massachusetts residents as required pursuant to G.L. c. 93H, § 3.

11. SSH shall report data breaches involving PHI to the Office for Civil Rights for the U.S. Department of Health and Human Services and provide proper notice of data breaches to individuals in compliance with HIPAA.
12. SSH shall comply fully with 201 C.M.R. 17.00, including by:
    a. implementing, maintaining, and adhering to a WISP;
    b. producing its most recent WISP to the Commonwealth within fourteen (14) days after the date of entry of the Final Judgment;
    c. reviewing its security measures annually;
    d. training its workforce at least once every 12 months on proper data security, including proper disposal of paper and electronic media containing PI or PHI, and proper reporting of data security incidents;
    e. providing written reminders once every 12 months to its employees with contracting authority regarding proper procedures for obtaining B.A. or Service Provider agreements with third-parties; and
    f. requiring its B.A.s and Service Providers by contract to implement and maintain appropriate security measures to protect PI, consistent with state and federal regulations.
13. SSH shall not disclose PI or PHI to any B.A. or Service Provider without taking reasonable steps to select and retain B.A.s or Service Providers capable of maintaining appropriate security measures.

14. SSH shall, prior to entering into any new agreement with a B.A. or Service Provider, or upon the next renewal (for agreements with a defined term) or upon amendment due to a material change in services or a material changes in one or more Laws Related to Data Security (for evergreen agreements) of existing B.A. or Service Provider agreements:
    a. inquire about the B.A's or Service Provider's methods for ensuring safeguards are in place to protect PI and PHI;
    b. inquire about the B.A.'s or Service Provider's methods for disposing of PHI and PHI;
    c. inquire about the security of the B.A.'s or Service Provider's facilities to understand the types of physical safeguards and methods used by the B.A. or Service Provider to protect PI and PHI;
    d. inquire about the B.A.'s or Service Provider's training of its employees regarding the requirements for handling or disposing of PI or PHI pursuant to state and federal law; and
    e. request a copy of the Service Provider's WISP.
15. With respect to those B.A.s and Service Providers SSH engages for the purpose of providing data destruction services, SSH shall
    a. Prior to entering into any new agreement or within sixty (60) days of the Effective Date for existing agreements:
        i. obtain and review a copy of the B.A. or Service Provider's WISP;

ii. request a copy of policies and procedures delineating the B.A. or Service Provider's PI or PHI disposal methods;

iii. obtain assurances that PI is destroyed pursuant to the requirements of G.L. c. 93I;

iv. require the B.A. or Service Provider to obtain SSH's consent before engaging an agent or subcontractor to carry out any duties related to destruction of PI or PHI;

v. either (A) require the B.A. or Service Provider to agree in writing that the B.A. or Service Provider requires any permitted agent or subcontractor to be bound by the same types of restrictions, terms, and conditions concerning the protection of PI and PHI that apply to the B.A. or Service Provider, or (B) enter into a direct B.A. or Service Provider Agreement with the agent or subcontractor;

b. request certificates of destruction from the B.A. or Service Provider upon destruction of SSH's PI or PHI promptly, and at least within 90 days after the destruction was scheduled to have taken place, and review certificates of destruction if provided to SSH; and

c. maintain documentation which shows that SSH has complied with the obligations set out in Sections 13, 14, and 15.

16. SSH shall:

a. maintain a current list or lists reflecting all of its B.A.s and Service Providers;

b. obtain written B.A. agreements or Service Provider agreements from each B.A. or Service Provider;

c. maintain a written copy of all B.A. agreements and Service Provider agreements and ensure that all such agreements are submitted to SSH before any PI or PHI is transferred to a B.A. or Service Provider; and

d. review existing B.A. and Service Provider agreements upon the next renewal (for agreements with a defined term) or upon amendment due to a material change in services or a material change in one or more Laws Related to Data Security (for evergreen agreements).

17. SSH shall develop template B.A. or Service Provider agreements containing language requiring its B.A.s and Service Providers to:

a. encrypt and destroy PI and PHI as required by one or more Laws Related to Data Security, as applicable, including requiring all PI stored on laptops or other portable devices to be encrypted; requiring all records and files containing PI transmitted across public networks and/or transferred wirelessly to be encrypted; and requiring all PI to be destroyed pursuant to the requirements of G.L. c. 93I, provided that SSH shall negotiate for similar language when using the B.A. or Service Provider's form of agreement; and provided further that, absent agreement to a specific reference to such Laws Related to Data Security, SSH shall negotiate to include a provision requiring the B.A. or Service Provider to represent that it complies with federal and Massachusetts law; and

b. report all data breaches to SSH involving the PI or PHI created or maintained on behalf of SSH, and work with SSH so that the data breach is reported in a timely manner to proper state and federal authorities.

18. SSH shall produce to the Commonwealth a template B.A. agreement and template Service Provider agreement within thirty (30) days of the Effective Date.

19. SSH shall:

a. within three (3) months of the Effective Date, engage a third-party firm to review and audit:

i. SSH's compliance with the Federal Standards for Privacy of Individually Identifiable Health Information (45 CFR §§ 160 and 164) and 201 CMR 17.00, in each case as they pertain to data destruction;

ii. SSH's WISP, and SSH's compliance with its WISP as it pertains to data destruction, the encryption of PI on portable devices, the encryption of PI transmitted across public networks and/or transmitted wirelessly, and the selection of B.A.s or Service Providers engaged by SSH for the purpose of providing data destruction services; and

iii. all agreements with B.A.s that are engaged by SSH for the purpose of providing data destruction services;

b. take all corrective actions recommended in the compliance review that are necessary to bring SSH in compliance with state and federal law; and

c. provide a written report to the Commonwealth as to the results of the compliance review and the corrective actions SSH takes as result of the compliance review.

20. Within sixty (60) days of the Effective Data, SSH shall encrypt, erase, or destroy, to the extent technically feasible, all PI in its possession that is contained on portable devices to the extent required by Massachusetts law. SSH shall not be required to encrypt PI on back-up tapes created prior to March 1, 2010.

21. To the extent that one or more terms set forth in Sections 12, 14, 15, 16, or 17 above conflict with or become otherwise inconsistent with enhanced requirements set forth in subsequent amendments to Laws Related to Data Security, the enhanced requirements of such Laws Related to Data Security, as amended, or such other applicable laws as may be implemented, shall govern for the purpose of determining SSH's compliance with the Consent Judgment. If SSH and the Commonwealth disagree as to whether the Consent Judgment or the amendments to Laws Related to Data Security following the Effective Date govern, SSH and the Commonwealth shall in good faith attempt to resolve their differences. If SSH and the Commonwealth cannot resolve their differences, either party may give written notice that it intends to seek judicial review. The Massachusetts Superior Court, sitting in Suffolk

County, retains jurisdiction of this action for the purpose of enforcing or modifying the terms of this Consent Judgment, or granting such further relief as the Court deems just and proper, and the provisions of this Consent Judgment shall be construed in accordance with the laws of the Commonwealth of Massachusetts.

22. Within ten (10) days after the entry of this Final Judgment by Consent, SSH shall cause a true and correct copy of the injunctive terms contained herein to be given to every person who on the date of entry of this Consent Judgment is an officer or a member of the board of directors of SSH.

23. SSH shall comply with all reasonable inquiries and requests from the Office of the Attorney General regarding implementation of the terms contained within this Final Judgment.

IV. PAYMENT

24. Pursuant to G.L. c. 93A, judgment is entered against SSH in the amount of $750,000.

25. Upon entry of a Final Judgment in this matter, SSH shall pay (i) $250,000 to the Commonwealth as civil penalties and (ii) $225,000, pursuant to G.L. c. 12 § 4A, as a contribution to a fund to be used at the sole discretion of the Attorney General, to promote education or further investigation/litigation in the area of PI and PHI data protection or to fund other programs, such as a local consumer aid fund, reasonably targeted to benefit consumers.

26. In satisfaction of the remainder of the judgment, the Commonwealth shall credit SSH $275,000 for security measures instituted by SSH to improve the protection of PI and PHI in its possession.

27. Payment shall be made by SSH by certified or cashier's check made payable to the "Commonwealth of Massachusetts" and delivered to Shannon Choy-Seymour, Assistant Attorney General, Consumer Protection Division, One Ashburton Place, Boston, Massachusetts 02108.

V. NOTICES

28. All notices and documents required by this Final Judgment shall be provided in writing to the parties as follows:

A. If to the Attorney General:

Shannon Choy-Seymour (BBO# 663245)
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
(617) 727-2200, ext. 2918
Shannon.Choy-Seymour@state.ma.us

Lois Johnson (BBO# 636151)
Assistant Attorney General
Health Care Division
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
(617) 727-2200, ext. 2054
Lois.Johnson@state.ma.us

B. If to South Shore Hospital, Inc.:

Mark E. Robinson, (BBO# 423080)
Siobhan E. Mee (BBO# 640372)
Bingham McCutchen, LLP
One Federal Street

Boston, MA 02110
(617) 951-8000
siobhan.mee@bingham.com

Christine G. Savage (BBO# 629671)
Julia R. Hesse (BBO# 655572)
Choate, Hall & Stewart, LLP
Two International Place
Boston, MA 02110
(617) 278-5000
csavage@choate.com
jhesse@choate.com

VI. WAIVER OF APPEAL AND OF FINDINGS AND RULINGS

29. SSH waives all rights of appeal and also waives the requirements of Rule 52 of the Massachusetts Rules of Civil Procedure with respect to entry of this Final Judgment.

VII. MISCELLANEOUS

30. Compliance with this Final Judgment resolves and settles all civil claims the Commonwealth has or may in the future have against SSH relating to the allegations, facts and circumstances set forth in the Complaint filed against SSH in this action.

31. The provisions of this Final Judgment shall be severable and should any provisions be declared by a court of competent jurisdiction to be unenforceable, the other provisions of this Judgment shall remain in full force and effect.

32. Nothing in this Final Judgment shall be construed as relieving SSH of its duty to comply with all applicable federal, state, and local laws, regulations, rules, and permits.

33. Consent to this Final Judgment does not constitute an approval by the Commonwealth of any of SSH's business acts and practices.

34. Except for purposes of enforcement of this Final Judgment by the Commonwealth or by Court order, no part of the Complaint or this Final Judgment shall be admitted into evidence against SSH or any of its parent corporations, subsidiaries, officers, directors, employees, predecessors, successors, and assigns. No allegation or assertion of liability or wrongdoing on the part of SSH, set forth in either the Complaint or the Final Judgment, shall be treated or construed as an admission of liability or wrongdoing by SSH or any of its parent corporations, subsidiaries, officers, directors, employees, predecessors, successors, or assigns.

35. Any violation of this Final Judgment is punishable by civil contempt proceedings, or as otherwise provided by law.

36. This Final Judgment becomes effective upon entry by the Court, and all periods of time described herein commence as of that date.

APPROVED AND ORDERED:

_____

Justice of the Superior Court

Dated: _____, 2012

CONSENT TO JUDGMENT OF SOUTH SHORE HOSPITAL, INC.

1. The Defendant, South Shore Hospital, Inc. ("SSH"), admits to the continuing jurisdiction and venue of the Suffolk Superior Court, and hereby consents to the entry of the Final Judgment in the form attached hereto. In so consenting, SSH certifies that it has read and understands each of the sections, paragraphs, and subparagraphs in the Final Judgment.
2. SSH waives the entry of findings of fact and conclusions of law pursuant to Rule 52 of the Massachusetts Rules of Civil Procedure.
3. SSH understands that the obligations set forth in the Final Judgment apply to SSH and its predecessors, successors, and assigns.
4. SSH states that it understands that any violation of this Final Judgment may result in sanctions against it under G.L. c. 93A, § 4, and/or a finding of contempt of court.
5. SSH states that it is represented by legal counsel, and that Richard Aubut, President of SSH, has personally read and understands each numbered paragraph in the Final Judgment by Consent.
6. The undersigned, Richard Aubut, represents that he is duly authorized to execute this Consent to Judgment on behalf of SSH and to bind SSH to all of its provisions, and that on behalf of SSH he voluntarily enters into this Final Judgment by Consent.
7. Except for purposes of its enforcement, this Consent shall not constitute evidence against SSH.

ASSENTED TO, WAIVING ALL RIGHTS OF APPEAL

BY: _____ Dated:

Richard Aubut, President
South Shore Hospital, Inc.