STATE OF CONNECTICUT
OFFICE OF THE ATTORNEY GENERAL

In the Matter of	)	
Hartford Hospital,	)	**ASSURANCE OF VOLUNTARY COMPLIANCE**
VNA HealthCare, and	)	
EMC Corporation	)	
	)	

The Office of Attorney General of the State of Connecticut has conducted an investigation into the loss of data (the "incident") by a contractor of Hartford Hospital and VNA HealthCare, Inc. (together, the "Hospital"), EMC Corporation ("EMC"; together with the Hospital, the "Parties"). The investigation examined the facts and circumstances surrounding the incident and examined whether the Parties complied with the Health Insurance Portability and Accountability Act ("HIPAA") and state law. The Parties and the Attorney General wish to enter into this Assurance of Voluntary Compliance ("AVC") to resolve all issues arising out of or relating to the incident.

IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AND THE ATTORNEY GENERAL THAT:

1. On or about December 28, 2011, the Hospital engaged EMC to assist the Hospital on a quality improvement project relating to analyzing patient data for the purposes of reducing the incidence of avoidable hospital admissions associated with congestive heart failure (the "Project").

2. On June 25, 2012, an unencrypted laptop in the possession of an EMC employee was stolen from the employee's home. The employee had been employed by and received the laptop that was stolen from a company that EMC had previously acquired.

3. The laptop contained the unencrypted protected health information ("PHI"), as defined in the Health Insurance Portability and Accountability Act and regulations promulgated thereunder (45 C.F.R. § 160.103), and/or personal information (*see* Conn. Gen. Stat. §§ 36a-701b and 42-471) of approximately 8,883 Connecticut residents relating to the Project.

4. Upon discovering the theft of the laptop, EMC reported the laptop theft to the local enforcement authorities. Despite an investigation by EMC and others, and a search for the laptop, the laptop has not been recovered.

5. On or about June 26, 2012, EMC notified the Hospital of the theft of the laptop.

6. Upon receiving notice of the laptop theft from EMC, the Hospital determined that it had not entered into a Business Associate Agreement ("BAA") with EMC.

7. Although the laptop has never been recovered, the Hospital represents that it has no evidence that any of the PHI or other personal information has been misused.

8. The Hospital notified the Office of the Attorney General of the stolen laptop on July 13, 2012, and the Attorney General's Office thereafter commenced an investigation into the incident.

9. In July 2012, the Hospital engaged AllClear ID to offer credit monitoring services and identity theft insurance coverage for those patients whose PHI was contained on the stolen laptop.

10. On or about July 30, 2012, the Hospital sent notification letters to the patients whose PHI was contained on the stolen laptop. The Hospital also issued a media statement, which was posted on its official web site to give public notice of the laptop theft.

11. In addition to the steps taken by the Hospital that are summarized above, the Hospital also has undertaken the following corrective measures, which particularly focus on HIPAA requirements relating to BAAs:

a. The Hospital's Privacy Officer has provided remedial education (which included significant focus on requirements relating to business associates) to the individuals who were responsible for obtaining a BAA with EMC for the Project;

b. The Hospital has developed a Business Associate and Privacy & Information Security Vendor Contract Flowchart to assist business managers in determining when a BAA is required;

c. For contracts entered into by the Information Technology ("IT") department, the Hospital has developed and implemented an IT Contract Checklist and a Privacy and Security Pre-Contract Questionnaire. The IT Contract Checklist assists business managers in IT in identifying the types of PHI to be shared with the vendor in order for the vendor to perform its duties and in determining whether a BAA is required. The Questionnaire assists the information security staff in evaluating whether a potential business associate with electronic access to Hospital data meets minimum privacy and security controls for handling PHI;

d. The Hospital has enhanced annual mandated compliance training for the Hospital workforce to include greater emphasis on the legal obligations relating to business associates and having valid BAAs;

e. The Hospital has developed a new training/awareness module for Hospital business managers in connection with their HIPAA obligations related to business associates and established an annual training requirement for business managers who have the authority to enter into contractual relationships;

f. As part of the Hospital's contract review and approval process for the IT department and supply chain contracts, the business manager's determination of whether a BAA is needed and if so whether such an agreement is in place is reviewed by the supply chain contract administrator, the IT contract administrator, the Privacy Officer, or the legal department; and

g. The Hospital has created new contract templates for Supply Chain Management and IT agreements (i.e. vendor agreements) that incorporate the HIPAA required business associate provisions into the body of the contracts.

12. In addition to the foregoing, the Hospital shall, and to the extent it already has been doing so, shall continue to:

a. Comply with applicable provisions and standards under HIPAA.

b. Examine its present relationships with those business associates that have existing contracts for data analytics involving substantial access

to patient data in order to determine whether an appropriate and executed BAA for each such relationship is in place.

c. Pursuant to its security risk assessment, utilize a combination of hardware and software to encrypt files or data containing PHI prior to its transmission or transfer.

d. Require each employee to certify, in writing or in electronic form, that he or she has participated in the required annual privacy training (referenced in paragraph 11.d above) and the date training was completed, and retain all training course materials for two years for purposes of audits or reviews.

e. Include in future contract policy audits a review of whether a BAA is needed and in place.

f. Submit to the Attorney General's Office a report one year after this AVC is signed by the Parties, to demonstrate its implementation of the corrective action measures in this AVC, including relevant training and monitoring.

13. The Hospital will take reasonable steps to monitor and ensure compliance with this AVC and will retain documentation of its monitoring and compliance efforts related to this AVC for two (2) years and produce such documentation upon request of the Attorney General within thirty (30) business days of such a request.

14. EMC shall, and to the extent it has already, continue to:

a. Maintain reasonable policies and procedures requiring, if technically feasible, the encryption of all PHI stored on laptops or other portable devices and transmitted across wireless or public networks.

b. Maintain reasonable security policies for employees relating to the storage, access, and transfer of PHI outside of EMC premises.

c. Maintain reasonable policies and procedures for responding to events involving unauthorized acquisition, access, use or disclosure of PHI as appropriate.

d. Use reasonable efforts to apply all such policies and procedures to acquired subsidiaries as a condition for such entities handling PHI.

e. Provide regular employee training to inform employees who are responsible for handling and/or utilizing PHI in their work about their obligations under the law and EMC's policies with respect to protecting and securing PHI.

f. Periodically assess the effectiveness of EMC's internal controls related to protecting and securing PHI and implement updates to such controls based on those assessments as appropriate.

15. To resolve the alleged violations of HIPAA and other applicable laws arising out of or related to the incident, the Parties will make one payment to the State of Connecticut in the total amount of $90,000.00 (Ninety Thousand Dollars) payable to "Treasurer, State of Connecticut," to be deposited in the State of Connecticut General Fund. Such payment shall be made no later than ten (10) days after this AVC is signed by the Attorney General.

16. This AVC constitutes a voluntary resolution of all outstanding issues between the Office of the Attorney General and the Parties for alleged violations of HIPAA and other applicable state laws arising out of or relating to the incident occurring on or before the date this AVC was signed by the Attorney General.

17. This AVC will not be considered an admission by the Parties of any alleged violations arising out of or relating to the incident identified in this AVC for any purpose.

18. The Parties agree that any violation of the AVC may result in further enforcement action by the Office of the Attorney General.

19. The Parties hereto agree that amendments/modifications to the terms of this AVC, if any, shall be in writing and signed by a representative of each Party.

20. This AVC may be executed in counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart hereof and all of which together shall constitute one and the same document. One or more counterparts may be delivered by facsimile or electronic transmission or a copy thereof with the intent that it or they shall constitute an original counterpart hereof.

21. This AVC sets forth the entire agreement of the Parties, and there are no representations, agreements, or understandings, oral or written, between the Parties relating to the subject matter of this AVC that are not fully expressed herein.

WHEREFORE, the following signatures are affixed hereto:

HARTFORD HOSPITAL

By: _____ Date: 10-29-15

PRESIDENT, HARTFORD HOSPITAL

EMC CORPORATION

By: _____ Date: _____

GEORGE JEPSEN,
ATTORNEY GENERAL,
STATE OF CONNECTICUT

By: _____ Date: _____

Matthew F. Fitzsimmons
Assistant Attorney General

23926/6/3366494.3

HARTFORD HOSPITAL

By:_____ Date:_____

EMC CORPORATION

By: _____ Date: 11/2/2015
Elizabeth McCarron
Senior Vice President & Assistant Deputy General Counsel

GEORGE JEPSEN,
ATTORNEY GENERAL,
STATE OF CONNECTICUT

By: _____ Date:_____
Matthew F. Fitzsimmons
Assistant Attorney General

HARTFORD HOSPITAL

By:_____ Date:_____

EMC CORPORATION

By:_____ Date:_____

GEORGE JEPSEN,
ATTORNEY GENERAL,
STATE OF CONNECTICUT

By: _____ Date: 11-03-15
Matthew F. Fitzsimmons
Assistant Attorney General

23926/6/3366494.3