

## **Module 5 Activity: State of Connecticut Case Study-Corrective Action Plan**

**NOTE: The information in this handout comes directly from sections 25-48 of the Stipulated Judgment.**

**The State of Connecticut listed the following as the corrective actions in this case.**

UNITED STATES DISTRICT COURT  
DISTRICT OF CONNECTICUT  
ATTORNEY GENERAL OF THE  
STATE OF CONNECTICUT, and  
STATE OF CONNECTICUT  
Plaintiffs,  
v.  
HEALTH NET OF THE NORTHEAST, INC.,  
HEALTH NET OF CONNECTICUT, INC.,  
UNITEDHEALTH GROUP INC., and OXFORD  
HEALTH PLANS, LLC.  
Defendants.  
CIV. NO. 3:IOCV57(PCD)

### **CORRECTIVE ACTION PLAN**

25. Health Net shall be responsible for the performance of all of the steps in the following Corrective Action Plan. Because the Corrective Action Plan is being undertaken for all Health Net Members, certain steps required under the Corrective Action Plan will be administered through Health Net, Inc., but the obligations herein shall remain Health Net's sole responsibility.

### **ONGOING EFFORTS AND IMPROVED SYSTEMS AND CONTROLS**

26. In addition to any actions already undertaken, Health Net shall complete notification of all Health Net Members identified through the manual review process, including Connecticut members, whose PI or PHI was contained on the portable disk. Health Net shall complete this action by June 30, 2010.
27. Health Net represents that it has protected all newly identified Health Net Members by offering through Debix the following credit monitoring services for a period of two years from the date of their enrollment in the services: single bureau credit monitoring through Transunion; retroactive restoration assistance to the date of discovery of the portable drive loss (May 14, 2009); credit restoration services for any confirmed instances of identity theft Debix identifies; reimbursement for security freeze and to unfreeze credit (which is available for two years from the time the individual receives notification); and \$1,000,000 of Personal Internet Identity insurance.
28. Health Net shall supplement its existing security and privacy programs. Specifically, Health Net shall implement (in accordance with this Judgment) technological, training and personnel measures described below in order to further strengthen its security and privacy policies and practices to protect the PHI and PI of Health Net Members, including Connecticut members. It is expressly understood and agreed that regarding such improved systems and controls, the Attorney General does not endorse or approve any specific product or procedure, and that by agreeing to take such measures, Health Net does not admit that its policies or procedures were not compliant with HIPAA or other laws. Health Net shall complete/implement such actions by the dates specified below.

## **Module 5 Activity: State of Connecticut Case Study-Corrective Action Plan**

**NOTE: The information in this handout comes directly from sections 25-48 of the Stipulated Judgment.**

29. Health Net shall specifically utilize a combination of hardware and software that resides between the email server and the e-mail client, that is designed to identify email or attachments containing PHI or PI and automatically encrypt email containing such identified information prior to transmission. Health Net has implemented such actions as of September 24, 2009.
30. Health Net shall implement technology solutions designed to monitor, control and restrict the transfer of PHI and PI to removable media in accordance with applicable HIPAA standards. These technology solutions are designed to permit exceptions allowing transfers to removable media only after a valid business reason has been documented and submitted to Health Net for review and approved in accord with Health Net's policies. Health Net shall begin implementation of such actions by July 3, 2010.
31. Health Net shall utilize technology solutions designed to identify where PHI and PI reside on its systems and to log actual and attempted access to PHI and PI. Health Net shall also utilize technology solutions designed to log and identify when PHI/PI is uploaded or downloaded from a monitored desktop or laptop. Health Net shall begin implementation of these actions by October 1, 2010.
32. Health Net agrees to and acknowledges that it has implemented the encrypting of the hard drives on all company laptop computers. Health Net shall implement encryption on all Health Net desktop computers in the same manner. Health Net shall begin implementation of such encryption by July 3, 2010.

### **IMPROVED MANAGEMENT/OVERSIGHT STRUCTURE**

33. In addition to implementing the technologies designed to automatically encrypt information and disable unauthorized attempts to utilize removable media, Health Net shall strengthen its oversight of new IT projects as part of the effort to comply with applicable HIPAA security and privacy standards. Specifically, Health Net shall assign an Information Security Analyst ("ISA") to each new approved IT project. Health Net has implemented the ISA assignment requirement as of July 31, 2009.
34. The ISAs shall report directly to the Manager of Information Security and shall: (a) evaluate the security requirements at the outset of a new IT project; (b) check for security gaps during the IT project; (c) respond to project team inquiries regarding security requirements for the handling of PHI and PI and access control; (d) assess the security issues relating to any data migrations within an applicable IT project and (e) report security breaches to the Manager of Information Security.

### **IMPROVED TRAINING AND AWARENESS**

35. In addition to Health Net's existing policies and procedures governing privacy and security issues, Health Net shall undertake supplemental measures described below, which are designed to inform and educate its employees about the security and privacy requirements necessary to protect the PHI and PI of health plan members. Health Net shall require all Business Associates (as defined by HIPAA) to execute HIPAA compliant Business Associate Agreements, including confidentiality provisions that require the safeguarding of protected health information.
36. The Health Net Information Security team has developed process-specific training for all Health Net employees on encryption, storage and the removable media process. Health Net shall use its online Learning Management System to assign training and track compliance.

## Module 5 Activity: State of Connecticut Case Study-Corrective Action Plan

**NOTE: The information in this handout comes directly from sections 25-48 of the Stipulated Judgment.**

37. Health Net's Chief Information Officer (CIO) shall include information security as a regular agenda item at the "Monthly IT All Hands" meetings. Health Net shall undertake this action on an ongoing basis.
38. Health Net's IT department will continue to address a wide variety of information security topics in its monthly IT Awareness Newsletter that is sent to all Health Net employees. Health Net shall undertake this action on an ongoing basis.
39. In order to reinforce Health Net's Privacy Policies, on or about February, 2010, Health Net's Privacy Office provided all employees, a laminated one page information sheet about the policies and procedures governing the protection of PHI. Health Net shall provide all new employees with this laminated one page information sheet.
40. Health Net began to show DVDs at New Employee Orientation sessions beginning in February 2010 to all new Health Net employees (not just IT employees) with consistent training on their information security responsibilities. Health Net shall undertake this action on an ongoing basis.
41. All new Health Net employees will receive training regarding HIP AA privacy and security requirements including incident response procedures such as employee reporting mechanisms within Health Net (in addition to the information security training via DVDs mentioned above). Health Net shall undertake this action on an ongoing basis.
42. Current Health Net employees will receive annual HIPAA training to provide a continuing reminder of their responsibilities with respect to the security and privacy protection of PHI, including its proper use and disclosure. Health Net will electronically track completion of such HIPAA training. After 30 days, Health Net employees who have not completed such training will receive weekly reminders and will be identified as non-compliant in a monthly report sent to the Health Net Compliance department. Failure to complete training will adversely affect employees regarding performance goals specified in paragraph 44. Health Net will undertake this action on an ongoing basis.
43. Health Net's Director of Information Privacy will continue to coordinate an annual "Compliance Awareness Week" for all employees to emphasize the importance of protecting the privacy and security of **PHI**. In March, 2010, Health Net issued a Data Security Story on its intra net that consists of interviews with key members of its privacy and security teams to increase awareness among all employees of the serious consequences involved when **PHI** is not adequately protected. Health Net shall continue the annual "Compliance Awareness Week" on an ongoing basis.

### IMPROVING INCENTIVES, MONITORING, AND REPORTS

44. Health Net shall incorporate three new performance goals for all employees: a compliance goal--to run operations and businesses in accordance with all regulatory requirements; a privacy goal--to maintain working knowledge, understanding and full compliance with all Health Net privacy and security policies and procedures; and training goal--to complete all training required by law and Health Net policy. Health Net has implemented such performance goals effective January 1, 2010.
45. Within 120 days after the entry of this Stipulated Judgment, Health Net shall submit to the Attorney General's Office a written report on the status of all items in the Corrective Action Plan.
46. Should Health Net experience a security incident that qualifies as a breach under Conn. Gen. Stat. § 36a-701(b) which affects more than 500 Connecticut residents, Health Net shall provide the Attorney General's Office with written notice of such event within a reasonable time after discovery.

## **Module 5 Activity: State of Connecticut Case Study-Corrective Action Plan**

**NOTE: The information in this handout comes directly from sections 25-48 of the Stipulated Judgment.**

47. Beginning one year from the date the initial report referenced in paragraph 45 is provided; Health Net shall provide semi-annual updates to the initial status report. Commencing with the 2011 update, Health Net shall include a description of its monitoring activity regarding the Corrective Action Plan, a summary of findings, description of risks identified, and any recommendations to reduce such risks.
48. Upon reasonable request, Health Net shall provide such documentation regarding compliance with the Corrective Action Plan as may be requested by the Attorney General's Office within thirty (30) business days of such request. Health Net shall maintain for inspection and copying documents describing all technologies and products implemented pursuant to this Judgment and all Health Net policies and procedures, including amendments thereto, applicable to this Judgment. Such documents shall be maintained for a period of six (6) years.