

**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.,	:
UNITED HEALTH GROUP INC., and OXFORD	:
HEALTH PLANS, LLC.	:
Defendants.	:

Civ. No. \_\_\_\_\_

**COMPLAINT**

**I. PRELIMINARY STATEMENT**

1. Plaintiff Attorney General of the State of Connecticut, as *parens patriae* for the State of Connecticut and on behalf of the State of Connecticut in its sovereign capacity, institutes this action for injunctive relief, statutory damages, attorneys fees, and the costs of this action against defendants Health Net of the Northeast, Inc., Health Net of Connecticut, Inc., United Health Group, Inc., and Oxford Health Plans, LLC, for multiple violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, (hereinafter HIPAA), 42 U.S.C. §1302(a), and Department of Health and Human Services Regulations 45 C.F.R. §160 *et seq.*, and supplemental state-law claims under Conn. Gen. Stat. §§36a-701b and 42-110b, the

Connecticut Unfair Trade Practices Act (“CUTPA”) until a trial on the merits is held and final order is entered in this action.

## **II. JURISDICTION**

2. The jurisdiction of this court for the First Cause of Action is invoked pursuant to the HIPAA Act, 42 U.S.C. §1320d-5(d) and 28 U.S.C. §§1331.

3. Plaintiff Attorney General of the State of Connecticut has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. §1320-5(4).

4. This Court has supplemental jurisdiction pursuant to 28 U.S.C. §1367 over plaintiff’s state law claims.

## **III. PARTIES**

5. The plaintiffs are the Attorney General of the State of Connecticut, acting in his capacity as *parens patriae*, as provided under HIPAA, and the State of Connecticut represented by Richard Blumenthal, Attorney General, acting at the request of Jerry Farrell, Jr., Commissioner of Consumer Protection, pursuant to the authority of Chapter 735a of the General Statutes, Conn. Gen. Stat. §§ 42-110m(a) and 42-110o(b).

6. The defendant Health Net of the Northeast, Inc. is a domestic corporation duly licensed under the laws of the State of Connecticut and doing business within this state.

7. The defendant Health Net of Connecticut, Inc. is a domestic corporation duly licensed under the laws of the State of Connecticut and doing business within this state.

8. The defendant United Health Group Inc. is a Minnesota corporation licensed under the laws of the State of Connecticut and doing business within this state.

9. The defendant Oxford Health Plans LLC, a Delaware limited liability company licensed under the laws of the State of Connecticut and doing business within this state.

10. At all times relevant hereto, the defendants are and have been health plans within the meaning of HIPAA, 45 C.F.R. §160.103.

11. As health plans, each defendant is a covered entity within the meaning of HIPAA, and thus is required to comply with the HIPAA federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A, C and E of Part 164). These requirements include the obligation to maintain the security of protected health information, which is defined as individually identifiable health information that is transmitted by electronic media and maintained in electronic media within the meaning of HIPAA, 45 C.F.R. §160.103. These requirements include the duty to ensure the confidentiality, integrity, and availability of all electronic protected health information the defendant has created, receives, maintains and transmits. As a covered entity within the meaning of HIPAA, the defendants are further obligated to comply with the privacy regulations, under which the defendants may only use or disclose protected health information as expressly provided under HIPAA.

#### **IV. FACTUAL ALLEGATIONS**

12. On or about May 14, 2009, the defendant Health Net of the Northeast Inc. (hereinafter referred to as “Health Net”) learned that a portable computer disk drive that had been transported between California and Connecticut, containing protected health information (as that term is defined under HIPAA), social security numbers, and bank account numbers for approximately 446,000 past and present Connecticut enrollees disappeared from defendant Health Net’s Shelton Connecticut office.

13. Defendant Health Net took no action to promptly inform the plaintiff Attorney General’s Office, the State of Connecticut Department of Insurance, the State of Connecticut

Department of Consumer Protection, or any other Connecticut government agency authorities, regarding this missing protected health and other personal and private information.

14. Upon information and belief, the defendant Health Net, knowing that protected health information was subject to strict privacy and security protections of HIPPA, delayed and otherwise failed to properly and timely notify the plaintiff Attorney General's Office, or any other Connecticut government authorities, regarding this missing protected health and personal information.

15. Upon information and belief, the defendant Health Net subsequently learned that the computer disk drive containing the missing information pertained to approximately 446,000 individuals and comprised 27.7 million scanned pages of over 120 different types of documents such as insurance claims forms, membership forms, appeals and grievances, correspondence and medical records. Within these documents was contained personal information including names, addresses, social security numbers, protected health information and financial information such as bank account numbers. The foregoing protected health information and private information was not protected by encryption as that term is defined under HIPAA, 45 C.F.R. §164.304.

16. On information and belief, as reflected in a report issued by Kroll Inc., a computer forensic consulting firm retained by defendant Health, Kroll indicated that the data that was contained on the computer disk was not encrypted or otherwise protected from access and viewing by unauthorized persons or third parties, but rather was viewable through the use of commonly available software.

17. Based on information and belief, in particular the report of Kroll Inc., in deliberate disregard of its policies and procedures and requirements under federal law, the

defendant Health Net intentionally decided not to encrypt this private and protected health information.

18. Based on information and belief, in the process of creating the disk drive that contained protected health information, defendant Health Net did not create a log file of the collection and transfer of the data that was included on the disk drive. Accordingly, when the disk was discovered missing, the defendant Health Net's failure to create a log file further increased the risk of disclosure of the protected health information to unauthorized individuals and constituted a breach of the defendant's obligation to safeguard the protected health information because the defendant did not readily have information as to the contents of the disk drive. As a consequence, the defendant Health Net replicated the entire creation of the disk drive, thus delaying efforts to safeguard or otherwise mitigate the data breach.

19. Upon information and belief, the defendants did not notify Connecticut residents whose person information was, or was reasonably believed to have been, accessed by an unauthorized person through the Breach in any manner, including, but not limited to, written, telephone, electronic or authorized substitute notice until it posted a notice on its website on November 18, 2009 and began sending letters in a rolling mailing on November 30, 2009.

20. Upon information and belief, no law enforcement agency determined that the notification to affected Connecticut residents would have impeded a criminal investigation and requested that the notification be delayed.

21. Upon information and belief, the design and implementation of the defendant Health Net's purported policies and procedures regarding the security of protected health information were ineffective in appropriately and reasonably safeguarding protected health information.

22. Upon information and belief, the defendant Health Net failed to effectively supervise and train its workforce (including both employees and independent contractors) on the policies and procedures with respect to the appropriate maintenance, use, and disclosure of protected health information.

23. On or about December 2, 2009, the State of Connecticut Department of Insurance approved the acquisition and/or control of defendant Health Net of Connecticut Inc., and defendant Health Net of the Northeast, Inc. by defendants UnitedHealth Group Inc. and Oxford Health Plans LLC. As part of that approval, UnitedHealth represented to the Department of Insurance that it understood the serious nature of the data breach and that upon approval of the acquisition by the Department of Insurance, it was prepared to own the responsibilities and consequences that go along with having licensure of Health Net of Connecticut, including any obligations undertaken with regard to the data breach.

**V. FIRST CLAIM FOR RELIEF: VIOLATION OF THE HEALTH INSURANCE AND PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

24. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein and further alleges as follows.

25. Defendants each constitute a health plan and is thus a covered entity under HIPAA as defined by 45 CFR 160.103 and is thus subject to the security standards and privacy rules contained within the HIPAA. 45 CFR 164 Subpart A, C, and D.

26. By its actions alleged herein, Defendant Health Net and its successors and affiliated entities, defendant Health Net of Connecticut Inc., defendant Oxford Health Plans LLC, and defendant UnitedHealth Group Inc. violated HIPAA by failing to comply with the

standards, requirements, and implementation specifications as set forth in Part 160 and 164 of HIPAA including the following:

- a. Defendants failed to ensure the confidentiality and integrity of electronic protected health information it created, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1).
- b. Defendants failed to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).
- c. Defendants failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility to maintain their security in violation of 45 CFR 164.310(d)(1).
- d. Defendants failed to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).
- e. Defendants failed to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).
- f. Defendants failed to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).
- g. Defendants failed to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).
- h. Defendants failed to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(4).
- i. Defendants impermissibly and improperly used and disclosed protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502 *et seq.*
- j. Defendants failed to effectively train all members of its workforce (including independent contractors involved in the data breach) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).
- k. Defendants' policies and procedures establishing physical and administrative safeguards were not adequately designed to appropriately and reasonably safeguard protected health information in violation of 45 CFR 164.530(c).
- l. Defendants did not maintain an effective and appropriate sanctions policy for members of its workforce (both employees and independent contractors) who failed to comply with the policies and procedures for the protection and

safeguarding of protected health information in violation of 45 CFR 164.530(e).

**VI. SECOND CLAIM FOR RELIEF: UNFAIR TRADE PRACTICES IN VIOLATION OF CONN. GEN. STAT. §42-110b**

27. Plaintiff State of Connecticut incorporates by reference all preceding paragraphs as if fully set forth herein and further alleges as follows.

28. Plaintiff is the State of Connecticut (hereinafter, the “State”), represented by Richard Blumenthal, Attorney General, acting at the request of Jerry Farrell, Jr., Commissioner of Consumer Protection, pursuant to the authority of Chapter 735a of the General Statutes, Conn. Gen. Stat. §§ 42-110m(a) and 42-110o(b).

29. The acts and practices alleged herein occurred in trade or commerce in the State of Connecticut.

30. The Breach, which compromised the personal information, including social security numbers, of Connecticut citizens constitutes a “breach of security,” as that term is defined by Conn. Gen. Stat. §36a-701b(a).

31. In the manner described herein, the defendants unreasonably delayed the disclosure of the breach of security of personal information within the meaning of Conn. Gen. Stat. § 36a-701b(b).

32. Pursuant to Conn. Gen. Stat. §36a-701b(g), the defendants’ failure to disclose the Breach following the discovery thereof on May 14, 2009, at the latest, to each Connecticut resident whose personal information was, or was reasonably believed to have been, accessed by an unauthorized person through the Breach constitutes an unfair trade practice pursuant to Conn. Gen. Stat. §42-110b enforceable by the plaintiff Attorney General of the State of Connecticut.

**VII. THIRD CLAIM FOR RELIEF: CIVIL PENALTIES FOR WILFULL VIOLATIONS OF CONN. GEN. STAT. §42A-110b**

33. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein and further alleges as follows.

34. Defendants engaged in the unfair acts or practices alleged herein willfully when they knew or should have known that their conduct was unfair in violation of Conn. Gen. Stat. §42-110b and therefore, are liable for civil penalties of up to \$5,000 per willful violation pursuant to General Statutes §42-110o(b).

**VIII. DEMAND FOR RELIEF**

WHEREFORE, plaintiffs demand judgment against defendants for relief as follows:

- a. To preliminarily and permanently enjoin the defendant from further such violations as provided under 42 U.S.C. §1320d-5(d)(1)(A).
- b. Statutory damages for all violations by the defendant as provided under 42 U.S.C. §1320d-5(d)(2).
- c. Enjoining the defendants from continuing the unfair acts or practices as complained of herein under Connecticut state law, Conn. Gen. Stat. §§36a-701b, 42-110b and 42-110m.
- d. An order, pursuant to Conn. Gen. Stat. §42-110(b), directing defendants to pay civil penalties of not more than \$5,000 for each willful violation of Conn. Gen. Stat. §42-110b(a).

