

Module 3 Activity: State of Connecticut Case Study - Security Rule Violations

NOTE: the information in this handout comes directly from the Complaint; Paragraph 26 has been amended to include only the alleged security violations; the list of alleged privacy violations was presented in Module 2.

After considering the fact pattern and discussing the Security Rule violations as a class, here is what the State of Connecticut listed as Security Rule Violations.

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 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

Module 3 Activity: State of Connecticut Case Study - Security Rule Violations

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).