Journal of Contemporary Health Law & Policy (1985-2015)

Volume 20 | Issue 2 Article 7

2004

The Health Insurance Portability and Accountability Act (HIPAA) Implementation via Case Law

Joan M. Kiel

ESSAY

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) IMPLEMENTATION VIA CASE LAW

Joan M. Kiel, Ph.D, C.H.P.S

Compliance with the Transaction and Code Sets, the first of eleven parts of the Health Insurance Portability and Accountability Act (HIPAA), was mandated on October 16, 2002.[1] Since that time, the Privacy Rule and Security Rule have set compliance dates of April 14, 2003, and April 20, 2005, respectively. Although healthcare providers, clearinghouses, and health plans have all expressed some displeasure with the time and expense of implementing the Act, HIPAA will serve to mitigate some situations that have occurred in regards to patient health information confidentiality, security, and privacy. Relevant case law will help to clarify implementation of HIPAA.

I. CASE LAW

A. *Arbster v. Unemployment Compensation Board of Review*[2]

Jeanne Arbster was a registered nurse for Forbes Health System in Pittsburgh, Pennsylvania. On March 16, 1996, Arbster's mother was admitted to Forbes Regional Hospital for orthopedic injuries related to a fall.[3] Arbster was not the nurse assigned to her Mother's care, yet she would provide "care" to her during her non-working hours, just as any family member would whether or not she was medical personnel. The mother allowed Arbster to play an active role for her during the hospitalization.[4] Her mother though did not give her daughter permission to access her medical records (the hospital requires written

1. 42 U.S.C. § 201 (2000).
2. Arbster v. Unemployment Comp. Bd. of Review, 690 A.2d. 805 (Pa. 1997).
3. *Id.* at 807.
4. *Id.*

permission from the patient for another to access the patient's records).[5]

Problems arose when Arbster discussed what her mother's physician thought was confidential information. How could Arbster have obtained this confidential information? She was only able to obtain this information by accessing the hospital's computers because as an employee she had access.[6] Other family members who provide "care" to a relative could not garner this information via the computer system; therefore, Arbster was accused of violating employment privileges. Second, in her official employment capacity as a registered nurse, she was not the caregiver for her mother and thus should not have used the computer system to access the information.[7] Jeanne Arbster was aware of the hospital personnel policy which forbade access to records except for patients under one's official care in an employment capacity. She claimed that although she knew the policy, she also knew of other employees who had accessed information regarding patients not under their care but who were not penalized.[8] Jeanne Arbster was terminated on April 14, 1996.[9]

Jeanne Arbster was denied unemployment compensation and appealed the decision.[10] The Forbes Health System reiterated its policy that "employees may only access the computer records for the purposes of performing their job responsibilities." [11] Because Arbster was not officially assigned her mother as a patient, yet provided care to her while off-duty, the ruling was upheld and her termination was attributed to willful misconduct. [12]

The HIPPA Privacy and Security Rule would uphold the given ruling. First, an Authorization to Disclose would have needed to be signed as Arbster was not the official caregiver of her Mother and therefore was not in a "treatment role."[13] The patient, via the Authorization to Disclose, instructs which persons may access the patient's health information. In addition, the patient can specify what information can be shared. Second, HIPAA follows the "minimum

5. *Id.* at 808.
6. *Id.* at 807.
7. *Arbster*, 690 A.2d at 807.
8. *Id.* at 808.
9. *Id.* at 807.
10. *Id.*
11. *Id.*
12. *See Arbster*, 690 A.2d at 809.
13. 45 C.F.R. § 164.508 (1996).

necessary" and "need to know" principles.[14] Under these principles, the persons accessing the patient health information (PHI) are given the minimum necessary information to complete the task at hand. Also, they are only given the PHI that they have a need to know to complete the task at hand, their job functions. Given that Jeanne Arbster was not in an official job role capacity, she did not have a need to know, and thus the minimum necessary amount of PHI that needed to be accessed was zero. The HIPAA Privacy Rule states that only those with an official need to know, as specified by the healthcare provider – here Forbes Regional Hospital – can access the minimum necessary information to accomplish the work tasks as specified by the provider.[15] Third, Forbes Regional Hospital dictates computer usage, a facet of the HIPAA Security and Privacy Rules. Computer access is viewed as an employment privilege and thus there is a responsibility and trust that comes with its usage. The organization dictates the relationship of the employment agreement to the computer usage, keeping in mind the HIPAA minimum necessary and need to know principles. For example, computer usage guidelines might include preventing employees from the following:

-Amending or deleting proprietary software;

-Using email for personal use;

-Sharing one's password to those without access;

-Printing information and removing it from the premises;

-Gaining illegal external access to the network.

Upon employment, the new employee would sign a "memorandum of understanding" covering computer usage. Forbes Regional Hospital did indeed have a policy which forbade employees from inappropriate computer access and use. Fourth, in relation to computer access, the HIPAA Security Rule, Workforce Security, mandates that HIPAA entities implement policies and procedures to prevent workforce members who do not have access to electronic protected health information from looking at it.[16] Employees such as Jeanne Arbster would be violating the HIPAA rule and thus be subject to sanctions. Fifth, to have the employee assume the liability for her behavior, upon employment she can be asked to sign a form

14. 45 C.F.R. § 164.502(b)(1) (1996).
15. 45 C.F.R. § 164.502(b)(1) (1996).
16. 45 C.F.R. § 164.308(a)(3)(i) (1996).

stating her understanding of her access privileges to patient health information. This "Access Form" would specify the employee's role and the patient health information that she has a need to know in the minimum necessary amount given her job functions. It would also have language concerning the importance of keeping the information private and secure, and the ramifications, such as loss of computer privileges to termination, if such was not done. The employee would then sign and date the form. It is recommended that the form be updated, at a minimum, at one's annual review.

Jeanne Arbster, although claiming to be delivering patient care, violated confidentiality, privacy, and security laws. Forbes Regional Hospital terminated Arbster's employment, but under HIPAA, she could face civil and criminal penalties.

B. *Ihekwu v. City of Durham, North Carolina*[17]

Patrick Ihekwu of Durham, North Carolina, sued the City claiming that because the City listed medical information about his positive HIV status in his file, he was denied employment.[18] Ihekwu began working for the city of Durham in 1990 as a parking garage attendant.[19] In 1994 he was promoted to a Records Keeper Specialist in the City's Record Management Division (RMD).[20] In 1997 Ihekwu and his fellow employees were told that the RMD was being decentralized and that a reduction in work force would occur.[21] Ihekwu was offered an interview for a Police Records Clerk position which he successfully did.[22] This led to a conditional offer of employment based on a background check which included his medical records.[23] Ihekwu refused to supply the City with his medical records and therefore the offer of employment was rescinded.[24]

Ihekwu asserted that confidential patient health information was already seen by others and used in the employment decisions (such as him being part of the reduction in work force). He felt that he did not

17. Ihekwu v. City of Durham, 129 F. Supp. 2d. 870 (M.D.N.C. 2000).
18. *Id.* at 874.
19. *Id.*
20. *Id.*
21. *Id.* at 875.
22. Ihekwu, 129 F. Supp. 2d. at 876.
23. *Id.*
24. *Id.*

need to supply the medical records as unknown city employees had obtained records of his prescriptions and conveyed this information to others working for the city.[25] The defendant, the City of Durham, North Carolina, argued that the medical information was held separately from the other personnel information and thus played no part in the employment judgment. The ruling was upheld in favor of the defendant.[26]

First, given that the City of Durham, North Carolina, is not a healthcare provider, health plan, or healthcare clearinghouse per se, the type of HIPAA entity arrangement that the City is would first need to be determined. Most likely, the City would qualify as a hybrid entity as its main function is not to be a healthcare provider, health plan, or healthcare clearing house, but rather its involvement in the access to, utilization of, and maintenance of individually identifiable health Information (IIHI) is a byproduct of its normal business operations. Second, under HIPAA, Ihekwu would have the right to authorize what information to disclose and which persons may receive disclosure, including information to potential employers.[27] Third, the City, who houses the individually identifiable health information, can distribute the "Notice of Health Information Practices" to each person for which it has IIHI. The Notice of Health Information Practices outlines how the City of Durham, or any holder of individually identifiable health information, will utilize the patient health information.[28] The Notice first defines "individually identifiable health information" and then lists both the rights of the individual and the rights of the entity. For example, the Notice would specify that individuals can request of copy of their information, and that they can request to amend the information that is inaccurate or incomplete. The Notice then names and describes numerous areas whereby individually identifiable health information can be shared. Examples include public health purposes, legal matters, and treatment, payment, and healthcare operations. Although the Notice does not mention employment situations, this document has served to educate the public on just what individually identifiable health information can be used for, where it can be sent, and most appropriately, what are the rights of access for the patient. Fourth, the HIPAA Security Rule mandates administrative safeguards,[29] physical safeguards,[30] and technical

25. *Id.* at 874.
26. *Id.* at 877.
27. 45 C.F.R. § 164.522(b)(1)(ii) (1996).
28. 45 C.F.R. § 164.520(a)(1) (1996).
29. 45 C.F.R. § 164.308 (1996).

safeguards.[31] With these three safeguards, "others," as quoted by Ihekwu, would not have had legitimate access to his HIV status and related health information.

C. *Burger v. Lutheran General Hospital*[32]

Doris Burger alleged that Lutheran General Hospital violated her patient's rights to privacy.[33] Doris Burger had filed a lawsuit against the hospital concerning her care while a patient. She alleged that the hospital violated her right to privacy by discussing her patient health information with the hospital's legal counsel.[34] The hospital claimed that since it created the patient health information, it had a right to it.[35] The hospital also asserted that because Doris Burger filed a lawsuit concerning hospital quality of care, it needed to look at her information to further prevent any per se quality of care occurrences.[36] Furthermore, the hospital claimed that it was in the "discovery phase" of the legal proceedings and thus needed to have access to the information.[37] The Court ruled in favor of the hospital, concluding that the hospital had a right to intra-hospital communications of patient information.[38] The hospital also cited the Hospital Licensing Act which allows a hospital's staff to communicate to the hospital's legal counsel information regarding patient care and legal suits.[39]

Under HIPAA, three issues emerge in relation to *Burger.* First, upon admission to the hospital, Doris Burger would have been presented with the hospital's Notice of Health Information Practices.[40] The Notice specifies what is patient health information, how the healthcare provider can utilize the patient health information, and the rights of the individual in regards to the patient health information. Burger would have read that patient health information can be

30. 45 C.F.R. § 164.310 (1996).
31. 45 C.F.R. § 164.312 (1996).
32. Burger v. Lutheran General Hospital, 759 N.E.2d 533 (Ill. 2001).
33. *Id.* at 537.
34. *Id.*
35. *Id.* at 546.
36. *Id.* at 546.
37. *Burger*, 759 N.E.2d at 548.
38. *Id.* at 556.
39. *Id.* at 535.
40. 45 C.F.R. § 164.520(a)(1) (1996).

disclosed for treatment, payment, and healthcare operations. Healthcare operations encompass quality of care issues, such as the complaint that Burger brought forth. In order for Lutheran General Hospital to operate as a quality healthcare provider, its staff needs to follow up on patient issues. Second, if Burger believed that the follow-up was not under healthcare operations, but she wanted an answer to her issue, she would have then needed to sign an authorization to disclose. The disclosure specifies what patient health information is to be shared, to whom, and for what purposes. Here, Burger could have specified exactly what information the hospital could have used in its fact finding. Third – although this is a bit of a "Catch-22" as Burger wanted her complaint investigated, yet she did not want her patient health information discussed – the hospital would follow the "minimum necessary" and "need to know" principles in flowing up on her claims. If no follow-up could be conducted, how then would Doris Burger's issue have been resolved?

To some HIPAA entities and consumers, The Health Insurance Portability and Accountability Act is confusing, subjective, and time-consuming. But with case law, one can tie theory to practice and demonstrate that familiar healthcare situations are comprehensible within HIPAA. *Arbster, Ihekwu,* and *Burger* enlighten the Act and provide examples that can be used in deciphering the Act.