Annals of Health Law

Volume 11
Issue 1 *2002*

Article 10

2002

The Business Associate Brain Teaser: A Look at Problems Involving the Business Associate Regulations under the Health Insurance Portability and Accountability Act of 1996

Randi Heitzman
Himan Straub, P.C.

The Business Associate Brain Teaser: A Look at Problems Involving The Business Associate Regulations Under The Health Insurance Portability and Accountability Act of 1996

*Randi Heitzman, J.D.**

I. INTRODUCTION

Approximately twenty years ago, a patient could visit a physician without the concern that any information he or she provided to the physician would be disclosed to a third person. This assurance was evidenced by the lack of notations that the physician would make when he or she provided services to the patient.[1] However, advances in medical technology in the past two decades spurred physician specialization, and physicians began delegating medical treatment to non-professional technicians.[2] Health information passed accordingly from general practitioners to specialists, who in turn passed it to non-professionals such as radiologists.[3] As a result of this information transfer, meticulous documentation of the details of a patient's condition became essential for effective treatment of patients.[4]

In addition to the interests of specialists and non-professionals in patient health information, other persons and entities began to assert business-related interests in obtaining the same information. Health care payors, managed care providers, and government agencies claimed their use of the health information was necessary to accurately determine what kinds of treatment would be covered under the appropriate health plan, whether

* Randi Heitzman graduated *cum laude* from Pace University School of Law in May, 2002 with a Certificate in Health Law. In September, Ms. Heitzman will be joining Hinman Straub, P.C. in Albany, N.Y. where she plans to practice in the health law field. Ms. Heitzman would like to thank Professor Gretchen Flint and Steven Imbriaco for their guidance in drafting this article.

1. A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of the Health Insurance Privacy and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 2-4 (2000).

2. *Id.* at 3.

3. The term "health information" includes not only information pertaining to an individual's health, but also his or her name, address, phone number and any other information that could be used to identify an individual. *See* notes 58-59 *infra*.

4. *Id.*

the treatment provided by physicians was necessary, and whether providers were committing fraud.[5] This demand placed administrative burdens upon health care providers and organizations, and as a result, they began to outsource their administrative and management functions.[6] Subsequently, health care blossomed into a complex industry where more than twelve million providers and 500,000 companies made up approximately one-seventh of the economy.[7] Within this complex system, nearly every participant had access to health information.

As these third parties increased their participation in the health care industry, disclosures of health information often occurred without the knowledge of the patient. Health information was routinely disclosed to accrediting organizations, medical information bureaus, pharmacies, and self-insured employers.[8] Although the disclosures were deemed necessary, there were very few rules that governed how the information could be transmitted and used by these third parties.[9] Pharmacies, for example, typically misused health information.[10] Pharmacies often received health information from insurance plans to determine whether the plan covered particular medication. What the pharmacies did with this information was not regulated, and often would be sold or used by the pharmacies for marketing purposes.[11] CVS, for example, made patient prescription records available to a direct mail company so the company could encourage the patients to refill their prescriptions and consider alternative treatment.[12] Although these solicitations did not directly harm the patients, they had no knowledge that CVS made these records available, and had no knowledge that CVS infringed upon the privacy of their health information.[13]

---

5. *Id.*
6. 65 Fed. Reg. 82462, 82466 (2000).
7. Robert E. Nolan Company, Inc., *Cost and Impact Analysis: Common Components of Confidentiality Legislation*, at 2 (Fall 1999), *available at* http://www.renolan.com/healthcare/privacy.htm [hereinafter "Nolan Report"].
8. 65 Fed. Reg. 82462, 82466 (2000).
9. JOY PRITTS, ET AL., *The State of Health Privacy: An Uneven Terrain*, at 24 (August 8, 1999), THE HEALTH PRIVACY PROJECT *available at* http://www.healthprivacy.org/newsletter-url2306/newsletter-url_list.htm?sectionHPP%20Resources (last visited June 26, 2002) [hereinafter "Health Privacy Project"].
10. Paul Starr, *Health and the Right to Privacy*, 25 AM. J. L. & MED. 193, 197 (1999).
11. *Id.*
12. *Id.*
13. *Id.*

As health information became increasingly more exchanged, the utilization of computers by health care providers and organizations increased. The use of computers not only improved the overall effectiveness of the health care system, but also magnified the misuse of health information.[14] Computers gave health care providers the tremendous advantages of improving accessibility of patient records and processing billing claims faster, which in turn lead to better treatment and more accurate diagnoses.[15] Storing information on computers also increased the government's ability to identify and treat those at risk for disease, conduct vital research, and detect fraud and abuse.[16] These advantages encouraged most health care providers and organizations to make the transition from paper to electronic media.[17]

The computerization of patient information, however, made health information easily accessible and a number of individuals were irreversibly harmed. For example, an employee at the Florida Health Department stole a computer disk containing the names of 4,000 people who had tested positive for HIV and sent it to two newspapers.[18] A banker who served on his county's health board used the health board's computer to cross-reference customer accounts with patient information and called due the mortgages of those individuals suffering from cancer.[19] New York Congresswoman Nydia Velasquez's medical records, which included her attempt at suicide, were faxed from a New York hospital to a newspaper.[20] A hospital employee's thirteen year-old daughter took a computer-generated list of patient names and phone numbers from the hospital when visiting her mother at work, and as a joke, called the patients and told them that they were diagnosed with HIV.[21] Highly publicized examples such as these caused consumers to become cynical of how their health information was used.[22]

14. Starr, *supra* note 10, at 196.

15. Veling W. Tsai, *Cheaper and Better the Congressional Administrative Simplification Mandate Facilitates the Transition to Electronic Medical Records*, 19 J. LEGAL MED. 549, 561-562 (1998).

16. 65 Fed. Reg. 82462, 82465 (2000).

17. Tsai, *supra* note 15, at 562.

18. Starr, *supra* note 10, at 197

19. *See also* 65 Fed. Reg. 82462, 82467 (2000).

20. *Id.*

21. *Id.*

22. Starr, *supra* note 10, at 194.

Even inadvertent misuses of health information caused the public to become more distrustful. Similar to the CVS example provided above, these kinds of misuses were not performed to intentionally harm the individuals injured by the actions.[23] Examples of such unintentional misuse include: a woman was inundated with offers for baby formula, mementos and children's books less than a week after she gave birth to a stillborn baby;[24] and a Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that previously owned the computer, including the customer names, addresses, social security numbers, and the medicine issued.[25]

As a consequence of the widespread mistreatment of health information, consumers began to feel that health care participants completely disregarded the privacy of their health information.[26] Consumers began to shield themselves from the misuse of their health information by lying to their doctors, providing inaccurate information and "doctor-hopping."[27] Patient advocates found that without trust in the health care system, patients' health conditions would likely go untreated and public health initiatives would be compromised.[28]

The lack of trust in the health care system, along with the reports of widespread misuse of information, caused the federal government to evaluate the privacy of health care information. In 1998, the Health Privacy Project was launched by Georgetown University to provide the government with an overview of the privacy statutes enacted in each state.[29] The project determined that the current patchwork of laws did not provide comprehensive protection for health information, and it enabled information to be used or disclosed without notice to the individual and without the individual's consent.[30] In addition, most

23. *Id.* at 197.

24. Lois M. Collins, *Rx for Privacy*, DESERET NEWS, Sept. 2, 2001, at A01.

25. 65 Fed. Reg. 82462, 82467 (2000).

26. *Id.* at 82464.

27. *Medical Records Privacy: Testimony before the U.S. Senate Committee on Health Education Labor and Pensions on Medical Records Privacy and the Proposed Federal Regulation* (2000) (statement of Janlori Goldman, Director of the Health Privacy Project Institute for Health Care Research), *available at* www.healthprivacy.org/usr_doc/33798.pdf [hereinafter "Janlori Goldman, Health Privacy Project, 2000 Testimony"].

28. *Id.*

29. *See generally* Health Privacy Project, *supra* note 9.

30. *Id.* at 9-11.

states did not or could not protect the information once it was disclosed, which enabled the entity that received the health information to use it for non-health care purposes.[31] For example, the project found that only two states restrict disclosures of health information to employers.[32] In addition, it found that once health information was released to an entity, few states regulated any re-disclosure made by that entity.[33]

The Health Privacy Project brought the need for more protection of health information to Congress' attention. Congress addressed this need in Section 264 of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[34] The purpose of HIPAA was to combat waste, fraud and abuse in the health care system, as well as to improve the system's efficiency.[35] Amid this legislation, Congress created an Administrative Simplifications statute, which was enacted in order to improve the overall efficiency and effectiveness of the health care system by encouraging the development of a simpler health care system.[36] Most health care providers and health plans used multiple formats to perform various health care transactions.[37] By developing national standards, the government sought to create one format for each type of transaction in an effort to relieve the administrative burden of multiple formats.[38]

Within the Administrative Simplification provisions, Congress addressed the issue of the protection of health information, which would be transmitted through its proposed simplified electronic system. Section 264 directed the Department of Health and Human Services ("HHS") to recommend standards that would protect the privacy of health information, and if Congress did not promulgate final regulations within three years after the enactment of HIPAA, HHS was to do so.[39] The recommendations had to "at least" address the rights that indi-

31. *Id.* at 24.

32. *Id.* at 32. The only two states that restricted disclosures of health information to employers were Connecticut and Maryland. *Id.* at 32. In addition, a recent survey found that 35% of Fortune 500 companies review employees' medical records before making promotion decisions.

33. Health Privacy Project, *supra* note 9, at 32.

34. 42 U.S.C. § 201 *et seq.* (1996).

35. *Id.*

36. *Id.* at § 1320d-2.

37. H.R. Rep. No. 104-496(I), at 70 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1869.

38. *Id.*

39. 42 U.S.C. § 1320d-2(c) (2001).

viduals would have with regard to their health information, the procedures by which they could exercise those rights, and the uses and disclosures of health information that should be authorized or required.[40] Ultimately, Congress failed to promulgate final regulations and the responsibility was placed upon HHS to finalize the regulations.[41]

HHS drafted detailed privacy regulations, which sought to increase consumers' trust in the health care system through a regulatory framework that would serve to protect their health information.[42] To facilitate this purpose, HHS created regulations that would generally govern contracts between health care organizations and third party organizations that performed their administrative and management functions.[43] These "business associate" regulations generally demanded that contracts with third parties contain reassurances that any health information disclosed or used by the third parties would not be disclosed in a way that violated the privacy regulations.[44] Although these regulations appeared to be necessary in order to regain consumer trust and protect the privacy of individual health information, they have reached a large number of organizations that would only come into contact with health information on sporadic occasions. The administrative and economic burdens associated with implementing the business associate regulations have been a source of contention and confusion among participants in the health care system since the time they were drafted.

This paper will explore the provisions that govern business associate contracts and the health care participants' responsibilities with regard to business associates under the privacy regulations promulgated by HHS. It will compare and analyze the draft regulations with the final regulations, and discuss the problems that covered entities have encountered in complying with the privacy regulations. Finally, this paper will conclude that the business associate regulations are too ambiguous and complex to achieve both HHS' goal of protection of privacy and Congress' goal of administrative simplification.

40. *Id.* at § 1320d-2(b)(1)-(3).

41. 65 Fed. Reg. 82462, 82470 (2001).

42. *See generally* 64 Fed. Reg. 59918 (1999) (proposed regulations) and 65 Fed. Reg. 82462 (2000).

43. 45 C.F.R. § 164.504(e) (2000).

44. *Id.*

II. Overview of the Privacy Regulations

A skeletal overview of the final HIPAA privacy regulations is necessary in order to appreciate the difficulties that health care participants have encountered in complying with the business associate regulations.

A. General Rule

In general, covered entities are prohibited from using and disclosing a person's health care information.[45] Covered entities can only use or disclose health information if it is permitted by the privacy regulations.[46] Any other use or disclosure is prohibited and can lead to civil or criminal penalties.[47]

B. Covered Entities

Covered entities include health care providers, health plans, and health care clearinghouses.[48] A "health care provider" under the regulations includes physicians, hospitals and ancillary providers.[49] The regulations only apply to those health care providers that transmit health information electronically.[50] A "health plan" under the regulation is defined as an individual or group health plan that provides or pays for medical care.[51] A "health care clearinghouse" is defined as an entity that processes or facilitates the processing of health information, or an entity that receives transactions in order to process or facilitate the processing of health information.[52] Many health care clearinghouses' activities involve the processing of enrollment applications and the payment of premiums. In order to be considered a health care clearinghouse, information derived from the enrollment applications or used during the payment of premiums must come from another covered entity.[53]

The covered entities targeted by the privacy regulations are not solely private individuals and organizations. The regulations extend to those federal and state health care providers and orga-

45. 45 C.F.R. § 164.502(a) (2000).
46. *Id.*
47. *See* 42 U.S.C. §§ 1320d-5 (2000) and 1320d-6 (2000) for civil and criminal penalties.
48. 45 C.F.R. § 164.104 (2000).
49. *Id.* at § 160.103 (definition of "health care provider").
50. *Id.*
51. *Id.* (definition of "health plan").
52. *Id.* (definition of "health care clearinghouse").
53. *Id.*

nizations that provide health services.[54] For example, a state agency that administers health care clinics would be considered a covered entity.[55] Therefore, the breadth of the statute is very inclusive.

C. *Information Subject to the Regulations*

The information subject to the privacy regulations is termed "individually identifiable health information" ("IIHI") and includes any demographic information that could reasonably be used to identify an individual.[56] A subset of IIHI is "protected health information." Protected health information ("PHI") is information that relates to the health matters of an individual and is transmitted electronically or kept in any other form (i.e., paper).[57] IIHI and PHI have been used interchangeably in the regulations, which implies that there is no real distinction between the terms. This paper will accordingly refer to this information collectively as "health information" unless the specific term is within a quotation or is necessary to clarify an issue.

Information that is de-identified is not covered by the privacy regulations.[58] Information is considered de-identified if experts conclude that identifying an individual is nearly impossible, or if all identifiers are removed from the information (i.e., name, address, dates, phone numbers, fax numbers, e-mail address).[59]

D. *Privacy Notice*

The privacy regulations require that covered entities provide a notice to individuals to whom services are provided.[60] The "privacy notice" must be written in plain language and describe how health information may be used or disclosed by the entity.[61] Its function is to alert individuals to their privacy rights, explain the covered entities' obligations with regard to health informa-

54. *Id.* (definitions of "health care provider," "health plan," and "health care clearinghouse" include individuals and organizations that administer state or federal funded programs).

55. 65 Fed. Reg. 82462, 82478 (2000).

56. 45 C.F.R. § 164.501 (2000) (definition of "individually identifiable health information").

57. *Id.* (definition of "protected health information").

58. *Id.* at § 164.502(d).

59. *Id.* at § 164.502(a).

60. *Id.* at § 164.520(a).

61. *Id.*

tion, and inform the individuals of all the ways in which their health information may be used.[62]

E. Use and Disclosure of PHI

In general, covered entities must obtain consents and authorizations from individuals in order to use and disclose their health information. Consents from individuals are required prior to providing treatment, providing or obtaining payment for health care, and performing various other health care operations.[63] Authorizations are required in order to use or disclose health information for any other reason, such as marketing, pre-enrollment underwriting, and disclosure of psychotherapy notes.[64]

Health information that the individual authorizes to be used or disclosed must be limited to the minimum amount of information that is needed to accomplish the purpose of the use or disclosure.[65] The only exceptions to this "minimum necessary" standard are when the information is being disclosed to a provider for treatment purposes, to the individual to whom the information relates, or to HHS.[66] An individual has the right to request an accounting of the uses and disclosures of his or her health information, which indicates that all uses and disclosures should be documented.[67]

F. Administrative Requirements

Covered entities must each appoint a privacy official as the person who will be responsible for the implementation of the privacy regulations.[68] Covered entities must also designate a contact person who will be responsible for receiving complaints and responding to inquiries about the privacy notice.[69] Covered entities must train their workforces on the privacy policies and procedures relating to the use and disclosure of health information, and must document such training as proof of compliance.[70] They must also institute an internal complaint policy, verify requests for disclosure, respond to requests by an individual, and

62. *Id.*
63. *Id.* at § 164.506(a).
64. *Id.* at § 164.508(a).
65. *Id.* at § 164.502(b).
66. *Id.* at § 164.502(b)(2)(i)-(v).
67. *See generally* 45 C.F.R. § 164.528 (2000).
68. 45 C.F.R. § 164.530(a)(1)(i) (2000).
69. *Id.* at § 164.530(a)(1)(ii).
70. *Id.* at § 164.530(b)(1)-(2).

refrain from intimidating, threatening or discriminating against any individual who exercises a right authorized by the regulations.[71]

G. *Exceptions*

There are various circumstances in which covered entities can use or disclose health information without the consent or authorization of an individual. For example, an authorization does not have to be obtained from an individual if the use or disclosure is for payment, treatment or other health care operations.[72] An authorization and consent are not needed prior to the use or disclosure of health information to law enforcement officials,[73] to public health oversight agencies,[74] to provide for the safety of an individual or the public,[75] to public health research facilities,[76] for purposes of national security,[77] and various services performed by a government agency that provides public health benefits.[78] Each of these exceptions have particular conditions that must be met in order for covered entities to use or disclose the information without authorization or consent.[79]

H. *Penalties*

Violations of the privacy regulations can result in civil and criminal penalties, which are the same for any violation of the Administration Simplification provisions. The civil penalty is $100 per violation with an annual maximum of $25,000 per violation.[80] Criminal penalties will be generally assessed against covered entities that knowingly and improperly disclose health information or obtain it under false pretenses.[81] There are three levels of criminal penalties that increase in severity as the action becomes more harmful. The penalties are as follows: $50,000 fine and up to 1 year of imprisonment for unlawfully obtaining

71. *Id.* at § 164.530(g).
72. If the covered entity is offering the patient direct treatment, and not referring him or her to another provider, only consent is needed. 45 C.F.R. § 164.506(a)(1)-(2) (2000).
73. 45 C.F.R. § 164.512(f)(1) (2000).
74. *Id.* at § 164.512(d).
75. *Id.* at § 164.512(j).
76. *Id.* at § 164.512(i).
77. *Id.* at § 164.512(k)(2).
78. *Id.* at § 164.512(k)(6).
79. *See generally* 45 C.F.R. § 164.512(f) (2000).
80. 42 U.S.C. § 1320d-5 (2000).
81. *Id.* at 1320d-6.

or disclosing health information; $100,000 fine and up to 5 years imprisonment for obtaining health information under false pretenses; and $250,000 and up to 10 years imprisonment for obtaining or disclosing health information with the intent to sell, transfer or use the information for commercial advantage, personal gain, or malicious harm.[82]

I. Business Associate Regulations

Tucked away in the privacy regulations, are the "business associate" regulations.[83] The regulations generally require covered entities to maintain contracts with all third party persons or organizations that perform services for covered entities or on their behalf.[84] Although the business associate regulations are a small part of the privacy regulations, they have had a large impact on covered entities that must comply with them.

III. The Development of The "Business Associate" Under HIPAA

When Congress vested the Department of Health and Human Services ("HHS") with the authority to promulgate final regulations to protect the privacy of health information under Section 264 of HIPAA, it did not explicitly instruct HHS to promulgate regulations that would reach all entities that could have access to health information. HHS' jurisdiction under HIPAA was seemingly confined to health care providers who transmitted health information electronically, health plans and health care clearinghouses ("covered entities").[85] It also appeared that the business associate regulations would be confined to only those third party organizations and individuals that worked in concert with covered entities. The final regulations, however, seemed to expand the reach of the regulations to those third party individuals and organizations that would come into contact with health information on very few occasions.

82. *Id.*
83. *See generally* 45 C.F.R. § 164.504(e) (2000).
84. *Id.* at § 164.504(e)(1).
85. Under Section 264(c)(3), the "standards with respect to the privacy of [health information] in connection with the transactions described in section 1173(a) of" the Administrative Simplification provisions were to be promulgated within two years. 42 U.S.C. § 1320d-2(c)(3) (2000). Section 1173(a) only applies to health plans, health care clearinghouses and health care providers. 42 U.S.C. § 1320d-1 (2000).

A. *Proposed Regulations*

Within the proposed regulations, third party organizations and individuals were termed "business partners," which appeared to create a category of organizations that had close working relationships with covered entities. A "business partner" was defined as "a person to whom a covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity."[86] In the preamble to the proposed regulations, HHS explained that the definition included those persons who received information from the covered entity to perform functions for the covered entity.[87] HHS provided examples of those who might fall with the definition, such as lawyers, auditors, consultants, data processing firms, third-party administrators, and billing agents.[88] It further explained that only those individuals or organizations to which health information was deliberately shared were considered business partners, and that employees of covered entities were not considered business partners.[89] Therefore, only those individuals or organizations that provided services in which health information was knowingly involved would have been considered business associates.

In addition to the definition of business partners, the proposed regulations required covered entities to obtain "satisfactory assurances" from their business partners that health information would not be further disclosed by entering into a contract.[90] The contract had to provide that the business partner would not use or disclose health information other than as permitted by the contract and the privacy regulations.[91] Essentially this meant that a business partner was prohibited from using or disclosing health information it obtained from the covered entity for its own purposes (i.e., marketing). The contract also had to provide that the business partner would develop and use appropriate safeguards to prevent the unlawful use or disclosure of health information; report to the covered entity any uses or disclosures not provided for by the contract; make available any

86. 64 Fed. Reg. 59918, 59933(1999).
87. *Id.* at 59947.
88. *Id.*
89. *Id.*
90. *Id.* at 60054.
91. *Id.*

health information to individuals who request it; make its internal practices and records relating the use or disclosure of health information available to HHS; and ensure that any subcontractors or agents that obtained health information agreed to the same restrictions as the business partner.[92] Covered entities were also responsible for taking "reasonable steps to ensure" that its business partners complied with the contract.[93] These mandatory provisions placed a duty on covered entities to actively monitor their business partners' activities.

A contract between a covered entity and a business partner also had to make those individuals whose health information was disclosed to the business partner a third party beneficiary of the contract.[94] A covered entity could terminate the contract if it determined that a business partner violated a term of the contract.[95] However, a covered entity violated the privacy regulations if it knew or reasonably should have known of a breach of the contract by the business partner and failed to take reasonable steps to cure the breach or terminate the contract.[96] Essentially, HHS created a third party right to sue a covered entity if a business partner breached the contract and stated that it would hold the covered entity liable for breaches by its business partners.

B. Criticism of Proposed Regulations

These proposed regulations drew three general themes of criticism by a number of covered entities: high compliance costs, administrative burden, and the possibility of increased litigation. First, covered entities were concerned about the large economic burdens that were created by the business partner regulations.[97] Within the preamble to the proposed regulations, HHS stated that compliance with the regulations would cost covered entities an estimated $3.8 billion over a five-year period.[98] Although HHS admitted that the estimation did not include the implementation of a number of regulations, it stated that it attempted

92. *Id.* at 60054-55.
93. *Id.* at 60054.
94. *Id.* at 60055.
95. *Id.*
96. *Id.*
97. *See generally* Jonathan P. Tomes, *HIPAA's Privacy and Security Regulations: Administrative Complication, Not Simplification*, 28 Health L. Dig. 11 (2000), *available at* http://www.healthlawyers.org/index.cfm (last visited Dec. 6, 2001).
98. 64 Fed. Reg. 59918, 60006 (1999).

to provide its "best estimate" based upon the limited data it could obtain.[99] In actuality, the regulations that HHS did not include in the estimation caused it to be substantially reduced. HHS' estimation did not include the costs of monitoring and assuming responsibility for business partners,[100] the costs of renegotiating contracts,[101] or the costs of liability associated with third party beneficiary lawsuits.[102] By not including these activities that were essential to compliance with the business partner regulations, HHS severely underestimated the economic burdens that covered entities faced.

Consequently, covered entities attacked HHS' estimation for its severe lack of inclusiveness. Throughout HHS' explanation of the costs, it repeatedly acknowledged that it did not include various regulations, and made explicit assumptions that national and state associations would develop model policies or guidelines that covered entities could adopt.[103] In calculating the estimate, HHS did not take into account that covered entities would have to implement policies that were tailored to their individual situations and such policies would have to be consistently reviewed in order to maintain compliance.[104] For example, Blue Cross Blue Shield testified before Congress that the $3.8 billion cost estimate was dramatically lower than the $43 billion cost that was projected in the Nolan Report, which was provided to HHS before it proposed the privacy regulations.[105] The American Hospital Association ("AHA") stated that HHS wrongly focused on costs that would have to be expended only once, whereas the policies and systems of the hospitals would require constant maintenance and updating.[106] The AHA illustrated that its hospitals spent an estimated $8.2 billion to ensure that their equipment was "Y2K compliant," and it would have to spend an equally inordinate amount to maintain compliance

99. *Id.* at 60007.

100. Eddy, *supra* note 1, at 39. *See also Medical Records Privacy: Testimony of the American Hospital Association before the Health, Labor and Pensions Committee of the U.S. Senate on the Administration's Proposed Rule on Medical Records Privacy* (2000) (statement of John Houston, American Hospital Assoc.) 2000 WL 19303008, at *6 [hereinafter "John Houston, AHA, 2000 Testimony"].

101. *Id.* at *3.

102. *Id.*

103. Tomes, *supra* note 97.

104. *Id.*

105. *AHIMA Calls Blue Cross Blue Shield $43 Billion Price Tag for Confidentiality Overblown*, HIPAAdvisory, *available at* www.hipaadvisory.com/views/Payer/BlueCrossStudyResponse.htm (last visited Dec. 6, 2001).

106. John Houston, AHA, 2000 Testimony, *supra* note 100, at *6.

with HIPAA.[107] In addition, a medical director of a large practice commented that the cost to comply with the "incredibly complex and convoluted" privacy regulations would be so "incredible" that the regulations would thwart any goal of improving patient accessibility to health care and the quality of care.[108] These arguments suggest that had HHS included the costs of implementing important regulations such as the business partner regulations, it would have drastically relaxed or changed the privacy regulations.

Closely related to the criticism of estimated compliance costs was the argument that the regulations would create a tremendous administrative burden. The health care providers and organizations argued that a large portion of the burden would stem from compliance with the business partner regulations.[109] Almost all third party businesses would have to comply with the privacy regulations through the contracts the covered entities were required to maintain, which meant all third party individuals or organizations would be subjected to audits by HHS.[110] In addition, business partners, as well as covered entities, would have to implement numerous policies and procedures in order to honor the contracts.[111] Virtually every participant in the health care industry would be tied up with administrative activities such as renegotiating contracts, enforcing compliance by employees, and monitoring their business associates.[112] Covered entities claimed that this "unrealistic and unworkable" activity would cause substantial disruption in the treatment of individuals and would impede patient/physician relationships.[113] Ultimately, covered entities argued that the burden created by the business partner regulations would contradict the intent of Congress to make the health care system more efficient.

HHS explained in the preamble to the proposed regulations that the purpose of the business partner contract provisions was

107. *Id.*

108. *Sampling of Comments on the Privacy Proposal: Providers*, HIPAAdvisory, *available at* http://www.hipaadvisory.com/views/Provider/ProviderComments.htm (last visited Dec. 21, 2001) [hereinafter "Sampling of Comments"].

109. *See e.g. Medical Records Privacy: Congressional Testimony Before the Senate Health, Education, Labor, and Pensions Committee* (2000) (statement of Charles Kahn, III, President, Health Insurance Assoc. of America), *available at* 2000 WL 19303005, at *6 [hereinafter "Charles Kahn, III, HIAA, 2000 Testimony"].

110. Eddy, *supra* note 1, at 65.

111. *Id.*

112. Charles Kahn, III, HIAA, 2000 Testimony, *supra* note 109, at *6.

113. Eddy, *supra* note 1, at 65.

to prevent covered entities from avoiding the regulations by contracting out many of their functions to third party individuals and organizations.[114] The functions or activities performed by the business partners are functions or activities that the covered entities could do themselves, and therefore, the business partners "stepped into the shoes" of the covered entities when they performed such functions or activities.[115] HHS also explained that business partners' activities should "be limited to the same extent as the covered entity for whom they are acting would be limited," and the business partner contract was the instrument through which such limitations should be placed.[116]

In addition, covered entities argued that the expanded scope of the privacy regulations only served to exacerbate the administrative burdens placed upon them. The definition of protected health information included health information kept either in electronic format, or "in any other form."[117] This meant that the health care providers and organizations would have to make attempts at protecting *all* health information, rather than only the information transmitted electronically.[118] The legislatively expressed purpose of the administrative simplification segment of HIPAA was to mainstream the use of electronic media and to create one electronic format for each type of electronic transaction, which in turn would make administrative tasks easier and more efficient.[119] By expanding the scope of the protected information to include all health information in any format, covered entities argued that HHS made it more difficult for them to implement policies to comply with the business partner regulations.[120]

For example, AHA argued that the inclusion of health information kept in paper format increased the burden of complying

114. 65 Fed. Reg. 82462, 82640 (2000). The preamble to the proposed regulations did not fully explain what HHS meant by "business partners." However, the preamble to the final regulations stated that HHS "retained the overall approach proposed" to the business partner regulations and that it somewhat expanded upon the purpose of the business partner regulations. *Id.* at 82504.

115. *Id.* at 82506.

116. 64 Fed. Reg. 59918, 59948 (1999).

117. *Id.* at 60053.

118. *AHA Comments on Privacy Regulation Proposal*, HIPAAdvisory (letter from Rick Pollack, Executive Vice President, AHA to Donna Shalala, Secretary of HHS), *at* http://www.hipaadvisory.com/views/Provider/ahacomment21700.htm (2000) (last visited Dec. 6, 2001) [hereinafter "AHA Comments on Proposed Regulations"].

119. H.R. Rep. No. 104-496(I), at 70 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1869.

120. John Houston, AHA, 2000 Testimony, *supra* note 100, at *3-4.

with the business partner regulations.[121] It argued that the business partner regulations effectively classified all business relationships its hospitals maintained with individuals and organizations outside of the hospitals as business partner relationships.[122] If health information kept in any form was subject to the privacy regulations, "business partners" would not only include any organization that based its functions on electronic transmissions, but also those organizations that based its functions on receiving or using paper documents.[123] Accordingly, not only would an organization that collects electronic data be a business partner, an organization that stores or shreds the medical records of a covered entity would also be considered a business partner.[124] Therefore, AHA argued that limiting the health information protected by the regulations to only electronically used or disclosed information would relieve the administrative burden placed upon the hospitals by eliminating the classification of a large number of organizations as business partners.[125]

Privacy advocates used the same argument that covered entities used in an attempt to persuade HHS to expand the scope of health information subject to the regulations. Janlori Goldman of the Health Privacy Project argued that expanding the scope of the protected information would eliminate any confusion as to how covered entities should treat paper records that contained electronically stored information.[126] Eliminating this confusion, she argued, would lead to easier implementation and reduce the administrative burden of covered entities accordingly.[127]

Unlike the arguments presented by covered entities, however, privacy advocates urged the expansion of the scope of health information in order to increase consumer confidence in the health care system.[128] They claimed that limiting the scope of the regulations to electronic information would give "consumers a false sense of security."[129] Consumers would only feel confidence in the system if they knew that *all* their health informa-

121. AHA Comments on Proposed Regulations, *supra* note 118.
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*
126. Janlori Goldman, Health Privacy Project, 2000 Testimony, *supra* note 27, at *4.
127. *Id.*
128. *Id.*
129. 65 Fed. Reg. 82462, 82618 (2000).

tion was protected and kept confidential.[130] Therefore, expanding the scope to include paper records was consistent with the bedrock purpose of the privacy regulations, which was to increase consumer trust in the system.[131]

The final problem that covered entities had with the proposed regulations, was the likelihood of increased litigation, which caused covered entities to be outraged. The mandate that required individuals to become third party beneficiaries to the business partner contracts, along with the penalty imposed against covered entities if they "should have known" of a breach of contract, implied that covered entities would be held responsible for the actions of its business partners.[132] Such liability required covered entities to actively monitor their business partners, which would be very costly and time-consuming.[133] Physician groups were particularly critical of the third party beneficiary provision because of their financial and administrative inability to monitor large national companies.[134] Some commentators suggested that penalties for a breach of contract by the business partners should only be imposed if covered entities had actual knowledge.[135]

C. Final Regulations

After reviewing numerous comments, HHS promulgated final regulations on December 28, 2000.[136] HHS changed two significant aspects to the regulations: the definition of protected health information, and the business partner regulations. HHS expanded the definition of protected health information to include all health information "maintained by a covered entity, regardless of form,"[137] despite the objections by covered entities that the proposed definition was over-inclusive. HHS agreed

130. Janlori Goldman, Health Privacy Project, 2000 Testimony, *supra* note 27, at *4.

131. *Id.*

132. Tomes, *supra* note 97; *see also* 65 Fed. Reg. 82462, 82640 (2000) (comments to the proposed business partner regulations).

133. *Id.*

134. *See* Sampling of Comments, *supra* note 108.

135. 65 Fed. Reg. 82462, 82640 (comments to the proposed business partner regulations); *see also Medical Records Privacy: Congressional Testimony before the Committee on Health, Education, Labor and Pensions United States Senate* (statement of Kathy Farmer, Hewlett Packard on behalf of Washington Business Group)(2000) *available at* 2000 WL 19303007, at *6-7.

136. *See generally* 65 Fed. Reg. 82462 (2000).

137. 65 Fed. Reg. 82462, 82496 (2000).

with the privacy advocates that the expanded definition would increase patient confidence in the health care system, and create more uniform standards in light of any confusion that would occur when records were both stored on a computer and kept in paper format.[138] In addition, HHS' underlying skepticism of participants in the health care system comported with its reasoning that an inclusive definition would eliminate an incentive for covered entities to only transmit information in paper format, and thereby, circumvent compliance with the regulations.[139]

Notwithstanding these valid reasons, HHS was careful in the way it structured the definition. Sensing possible legal consequences for this expansion, HHS crafted the definition in such a way as to keep it operational in case a court disagreed with the extent of HHS' authority.[140] HHS separated out the definition of protected health information to include information that was "(i) transmitted by electronic media; (ii) maintained in any electronic media. . .or (iii) transmitted or maintained in any other form or medium."[141] If a court disagreed with the extent of HHS' authority, it would only have to void section (iii) of the definition.

HHS also made significant changes to the business partner regulations. The obvious change was the substitution of the term "business associate" for the term "business partner."[142] The apparent purpose of the change in term was to achieve consistency with the regulations regarding electronic transactions that were promulgated prior to the privacy regulations.[143] Under the new rule, a person or organization would be a business associate if two circumstances existed: (1) if it performed, or assisted in the performance of, functions or activities that involved the use or disclosure of health information; or (2) if it provided services to or for a covered entity which involved the disclosure of health information.[144] The amount of health information used and/or disclosed would have to be "substantial" in

138. *Id.* at 82618.
139. *Id.* at 82619.
140. *Id.* ("We have structured the definition this way so that, if a court were to disagree with our view of our authority in this area, the rule would still be operational, albeit with respect to a more limited universe of information."); *see also* Mary Beth Johnston et al., *HIPAA Becomes Reality: Compliance with New Privacy, Security, and Electronic Transmission Standards*, 103 W. VA. L. REV. 541, 554-555 (2001).
141. 45 C.F.R. § 164.501 (2000) (definition of "protected health information").
142. 65 Fed. Reg. 82462, 82475 (2000).
143. *Id.*
144. *Id.* *See also* Johnston, *supra* note 140, at 562-63.

order for any person or organization to be considered a business associate.[145] This regulation opened up the possibility that covered entities (i.e., a clearinghouse) could be business associates of other covered entities (i.e., a health insurance company).[146] A person or an organization would not be considered a business associate if he or she was part of the "workforce" of a covered entity, if an organization was a subsidiary of a covered entity, if an organization was a financial institution that performs consumer financial transactions (i.e., clearing checks and processing credit cards), or if an organization acted as a conduit for health information.[147]

In addition to the definition change, HHS made changes to the business associate contract requirements. A major change was the removal of the third party beneficiary mandate.[148] HHS stated that it removed this requirement because some states' third party beneficiary laws provided for any responsibility that covered entities' owed to third parties.[149] HHS did not want to increase the complexity of these laws, nor did it want to affect the applicability of such laws.[150] Therefore, the third party beneficiary mandate was eliminated.

Another major change to the regulations was the apparent relaxation of the duty to monitor business associates. HHS removed the language that a covered entity must "take reasonable steps to ensure" that the business associate did not violate the contract, and added language that would require the covered entities to "cure a breach or terminate the contract. . . only if they know of a material violation."[151] A covered entity would "know" of a violation if it received "substantial and credible evidence" that a violation had potentially occurred.[152]

Despite HHS' relaxation of the monitoring requirement, a covered entity remains obligated to investigate every complaint and any other information that could contain substantial evidence of a violation.[153] If a covered entity determines that a

145. 65 Fed. Reg. 82462, 82507 (2000).
146. *Id.* at 82641 ("a covered entity must enter into a business associate contract with another covered entity when one is providing services to or acting on behalf of the other").
147. *Id.* at 82507.
148. *Id.* at 82505.
149. *Id.*
150. *Id.*
151. *Id.* at 82504.
152. *Id.*
153. *Id.*

violation occurred, it must cure the violation or terminate the contract, and the business associate would be required return or destroy the protected health information unless it is not feasible.[154] A covered entity would not have the option of maintaining the contract, even if it would be "convenient" for it to do so.[155] Therefore, it appeared that a covered entity would still be required to monitor its business associates.

HHS made an effort to clarify a number of the contract mandates. HHS explained that a business associate's obligation to ensure that its agents abide by the provisions of the business associate contract was only directed towards those subcontractors that essentially stepped "into the shoes of the business associate."[156] HHS did not intend to include any subcontractor that was not performing "business associate functions" (i.e., activities or services performed for or on behalf of the covered entity) or any subcontractor that, if it had directly contracted with a covered entity itself, would not give rise to a business associate relationship.[157] For example, if Law Firm contracts with Hospital to provide legal services for any malpractice claims that arise against Hospital, it will be considered a business associate of the Hospital. If Law Firm subsequently contracts with an architect to redesign its office, the architect would not be considered the type of subcontractor subject to the business associate contract Law Firm has with Hospital. The architect in this example is not "stepping into the shoes" of Law Firm by undertaking the task of providing legal services to Hospital. In addition, if the architect had directly contracted with Hospital to provide redesigning services, it would not give rise to a business associate relationship. Therefore, Law Firm would not have to ensure that the architect abides by the contract between it and Hospital.

HHS also sought to clarify when a business associate relationship would exist, and to eliminate interference with important and necessary transfers of health information. Primary care physicians that provided health information to specialized physicians were not considered business associates, and the transmission of such information was permitted without the consent or authorization of the patient.[158] An individual physician who worked at a hospital would not be considered a business associ-

154. *Id.* at 82505.
155. *Id.*
156. *Id.* at 82506.
157. *Id.*
158. *Id.* at 82504.

ate solely for the reason that the hospital granted him or her privileges.[159] Furthermore, an entity that was part of an affiliated network would not be considered a business associate.[160] Other exceptions included public health oversight agencies when they perform investigations and law enforcement officials when they carry out their legal functions.[161] It is important to note that although business associate contracts were not required under these circumstances, other privacy standards could apply.

HHS, however, maintained the rest of the business associate regulations. A covered entity was still required to include provisions that prohibited each of its business associates from further using or disclosing information other than as provided by the contract, which meant that business associates could not use health information for their own purposes.[162] The business associates would be required through the contract to develop and use safeguards against the unlawful use and disclosure of protected health information.[163] Each business associate contract still had to contain a description of the permissible uses and disclosures of health information, and require the business associate to report any uses and disclosures not provided for by the contracts to the covered entity.[164] The business associate contract had to require the business associate to make their internal practices, books and records available to the covered entities and HHS.[165] Lastly, the covered entity still had to obtain satisfactory assurances from the business associate that it would appropriately handle the information.[166]

159. *Id.* at 82476.

160. *Id.* at 82504.

161. *Id.* at 82505-506.

162. 45 C.F.R. § 164.504(e)(2)(ii)(A) (2000); *see also* 65 Fed. Reg. 82462, 82506 (2000) ("a business associate. . .that has business associate contracts with more than one covered entity generally may not use or disclose the protected health information that it creates or receives in its capacity as a business associate of one covered entity for the purposes of carrying out its responsibilities as a business associate of another covered entity, unless" the law states otherwise).

163. 45 C.F.R. § 164.504(e)(2)(ii)(B).

164. *Id.* at § 164.504(e)(2)(ii)(A), (C); *see also* 65 Fed. Reg. 82462, 82505 (2000) ("the contract must state the purposes for which the business associate may use and disclose protected health information.").

165. 45 C.F.R. § 164.504(e)(2)(ii)(H) (2000).

166. 65 Fed. Reg. 82462, 82505 (2000).

IV. Criticisms and Complications Remain

Although HHS attempted to clarify the business associate regulations, covered entities maintained their criticisms. They continued to be concerned about the enormous administrative burdens facilitated by the broad terminology used to define business associates. In addition, the possibility of increased litigation had not been alleviated by HHS' attempt to relax the monitoring requirements. Covered entities argued that the business associate regulations HHS maintained effectively required the covered entities to actively monitor their business associates. HHS' apparent lack of effort to ease these burdens has caused many covered entities to attack HHS' authority and make new demands of the agency.

A. Implementation Difficulties

Covered entities have argued that identifying the third party individuals and entities that would be considered business associates has created an administrative nightmare. This difficulty apparently stemmed from the sweeping terminology used to define business associates.[167] As stated above, the proposed rule would have defined business partners as a person or entity to whom protected health information was disclosed in order to perform a particular function or activity for the covered entity.[168] This definition implied that only when the covered entity deliberately provided health information to the third party entity would the third party be considered a business associate.[169] In comparison, the final definition included not only those persons and entities that actually obtain health information from the covered entities, but also those persons or entities that provide services to or for the covered entities "involving" health information.[170] The use of the word "involving" or "involves" by HHS and its expansion of the definition of business associates has caused profound affects upon the implementation of the business associate regulations.

One of the biggest problems encountered by covered entities has been determining which particular third party vendors

167. Tomes, *supra* note 97 ("the breadth of those subject to the standards is far greater than that in any previous law protecting the confidentiality of patient information").

168. 64 Fed. Reg. 59918, 59947 (1999).

169. *Id.*

170. 65 Fed. Reg. 82462, 82475. *See also* Johnston, *supra* note 140, at 562-63.

would be considered business associates. A covered entity, such as a hospital, usually contracts with numerous third party vendors, including organizations or persons whose services include software maintenance, medical device evaluations, equipment maintenance (i.e., printers, fax machines, etc.), interpretation for non-English speaking patients, shredding documents, and storing documents and data.[171] It is obvious that these vendors could occasionally obtain health information while performing their services for a covered entity, but does this indicate that the services provided for the covered entity "involve" the disclosure of such information?

HHS' failure to directly answer this question has resulted in covered entities taking two approaches to resolve this issue. The first approach is the "better to be safe than sorry" approach. This approach requires the covered entity to obtain a business associate contract (or add business associate language to a current contract) with all vendors that may have occasional access to protected health information.[172] For example, an organization that shreds documents for an insurance company may sporadically shred documents that include health information. If the insurance company utilizes the "better to be safe than sorry" approach, these services would "involve" health information. Accordingly, the insurance company would have to maintain a business associate contract with each third party organization that provides services in which it may occasionally come into contact with health information. This approach places a large administrative and economic burden upon the covered entity to identify each business associate and obtain a business associate contract from each entity.[173]

171. *See American Hospital Association Detailed Comments: Standards for Privacy of Individually Identifiable Health Information*, HIPAAlert (2001), *at* www.hipaadvisory.com/views/Provider/ahaDetail033001.htm (last visited Dec. 4, 2001) [hereinafter "AHA Comments on Final Regulations"].

172. Posting of William MacBain, wam@macbainandmacbain.com, to hipaalive@lists.hipaalert.com (Oct. 2, 2001) (copy on file with Annals of Health Law).

173. *See e.g., Testimony of the American Hospital Association before the Health, Education, Labor and Pensions Committee of the United States Senate on Making Patient Privacy a Reality: Does the Final HHS Regulation Get the Job Done* (statement of John Houston, Director, AHA) (2001) (undertaking the time-consuming task of reopening and negotiating business associate contracts contributes to the five-year cost of $ 22.5 billion for only hospitals, which is much more than the 10-year cost of $17.6 billion estimated by HHS for *all* covered entities), *at* www.aha.org/ar/Testimony/testprivacyB0208.asp. (last visited Dec. 6, 2001) [hereinafter "Houston, AHA, 2001 Testimony"].

The second approach requires each covered entity to thoroughly analyze the services provided by the vendors and conclude whether the vendor comes into contact with health information often enough to declare it a "business associate" for HIPAA purposes. HHS alluded to this approach in the preamble to the final regulations. It stated that third party individuals or organizations that "act merely as a conduit for protected health information" would not be considered a business associate.[174] HHS gave examples such as the U.S. postal services and private mail carriers, such as Fed Ex. It explained that conduits come across health information on an "infrequent and random basis" and accordingly, the risk of exposing health information to a conduit is very small.[175]

HHS further explained that only those persons or organizations that receive "substantial amounts" of health information from the covered entity would be considered a business associate.[176] Although "substantial amounts" imply quantity, the overall purpose of the privacy regulations implies that the type of information disclosed may also give rise to a business associate relationship.[177] For example, a covered entity that discloses names and addresses of patients on a daily basis to a third party may give rise to a business associate relationship because the cumulative amount of information being disclosed is large. However, a covered entity that provides a shredding service with documents that will occasionally contain the names and addresses of HIV-positive individuals may also give rise to a business associate relationship because protecting such information is very significant to the privacy of the individual.[178] Therefore, not only must covered entities identify their business associates under this approach, they must also clearly define the relationships they have with their business associates.

Although the latter approach appears to be the better approach, correctly determining whether an organization is a business associate could be difficult and covered entities will often

174. 65 Fed. Reg. 82462, 82476 (2000).
175. *Id.*
176. *Id.* at 82507.
177. One purpose of the privacy regulations was to prevent the shocking disclosures of information described in the Introduction (i.e., the employee at the Florida Dept. of Health that sent a computer disk containing the names of all those individuals who tested positive for HIV). These disclosures were isolated incidents, but the information that was disclosed was collectively important enough to encourage HHS to provide it protection.
178. *See* Eddy, *supra* note 1, at 12-16.

find themselves using the "better to be safe than sorry" approach anyway. For example, covered entities have questioned whether individuals that provide software maintenance, shredding services, and document storage are considered business associates.[179] Covered entities would have to review the services provided by these individuals and assess how much information is disclosed to them in order to determine if they are business associates.[180] A vendor that repairs only software containing medical information would likely be a business associate. Conversely, other software vendors may repair various programs, but only occasionally those programs could contain medical information. Covered entities would likely consider such software vendors to be business associates because of the possibility that the vendor may come across health information.[181] Even though "substantial amounts" of health information are not disclosed to such a vendor, the covered entities would consider the vendor a business associate because slightly more than "random and infrequent" disclosures will be made, and it would be better to err on the side of over-inclusiveness.

Problems could also exist in convincing vendors to comply with business associate regulations. Most vendors are not participants in the health care industry and do not regularly follow health care regulations. Covered entities could experience difficulty in persuading these third party vendors to take notice of the deadlines of compliance and make them comply on time.[182] In addition, the large vendors (i.e., AT&T) will not want multiple copies of business associate contracts that do not provide the same information. It is likely that these vendors would develop a standard business associate contract and would not negotiate on the language that is provided in the contracts, even though it

179. *See e.g.*, Posting of Dawn Martinez, dmartinez@infideni.net, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with Annals of Health Law); Posting of Edward Tinker, etinker@beaconpartners.com, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with Annals of Health Law).

180. Posting of altoby@aol.com to hipaalive@lists.hipaalert.com (Oct. 12, 2001) (copy on file with Annals of Health Law).

181. Posting of William MacBain, wam@macbainandmacbain.com, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with the Annals of Health Law).

182. *See e.g.*, Posting of Marvin Ottinger, marvin_ottinger@hotmail.com, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with Annals of Health Law).

may use or disclose health information in different ways for different covered entities.[183]

Although a covered entity could exercise the option of not contracting with such a vendor, some covered entities may be in a situation that would require them to maintain their services. For example, California requires its hospitals to have certified translators for health-related issues.[184] A family member of a patient is not considered "certified" under the law and cannot translate information from a hospital employee to the patient.[185] If the situation was an emergency, the hospital may need to quickly contact a translator service, such as AT&T interpreter services. The AT&T interpreter would translate the information to the patient for the employee over the phone. Under these circumstances, AT&T would need to have a business associate contract with the hospital and it may present the hospital with a standard contract.[186] If the hospital refuses to sign the contract the hospital may be without an interpreter. Such a "take it or leave it" attitude could place covered entities in precarious situations, because the covered entities would have to rely on a contract that was developed by a corporation that does not regularly follow health care regulations.

Apart from third party vendors, determining whether an entity is a business associate becomes even more complicated when intricate work relationships among covered entities are contemplated by the business associate regulations. For example, a clearinghouse may determine enrollment eligibility on behalf of an insurance plan.[187] The same clearinghouse may also negotiate the benefits of the plan with the insurance company on behalf of the potential enrollees. In the former situation, the clearinghouse would be considered a business associate, because it is performing a function on behalf of the plan that involves the

183. Posting of William MacBain, wam@macbainandmacbain.com, to hipaalive@lists.hipaalert.com (Sept. 21, 2001) (copy on file with Annals of Health Law).

184. Posting of Mara DeLaTorre, dehema@samc.com, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with Annals of Health Law).

185. *Id.*

186. *Id.*; *see also* posting of Marvin Ottinger, marvin_ottinger@hotmail.com, to hipaalive@lists.hipaalert.com (Sept. 20, 2001) (copy on file with Annals of Health Law).

187. *See e.g.*, Posting of William MacBain, wam@macbainandmacbain.com, to hipaalive@lists.hipaalert.com (Sept. 26, 2001) (copy on file with Annals of Health Law).

use of health information. In the latter situation, the clearinghouse would simply be considered a covered entity, because it is providing health care services directly to individuals in exchange for the payment of premiums. This example illustrates that each function of the clearinghouse would have to be meticulously analyzed in order to determine when it acts as a business associate and when it acts as a covered entity.[188] Parsing a covered entity's functions can be very difficult and time consuming.

Implementing the business associate regulations may cause difficulties for business associates as well. For example, a health plan may want to hire a review agency to review medical records of its enrollees who have visited hospitals and to make a recommendation on how the benefits provided by the health plan could be improved.[189] The review agency would be the business associate of the health plan because it is performing the review on behalf of the health plan. The review agency would not be a business associate of the hospital because it is performing no service for or on behalf of the hospital. Because the review agency is not a business associate of the hospital, the hospital cannot disclose any information to the agency without individual authorizations from the health plan enrollees.[190] Therefore, the reviewing agent might not be able to obtain the information it would need to perform the review on behalf of the health plan.

This situation becomes more complicated if the review agency has a business associate contract with the hospital, as well as the health plan. If the review agency in the above example has a contract with the hospital to provide a review and analysis of how the hospital needs to comply with HIPAA, the business associate regulations would require the contract to state that the review agency could only use the health information it obtains for the purposes of providing this specific service.[191] The review

188. *Medical Records Privacy: Congressional Testimony before the House Committee on Energy W.J. 'Billy' Tauzin, Chairman Subcommittee on Health Hearing Assessing HIPAA*, 107th Cong. (2001), *at* 2001 WL 2006326, *9 (statement of Bob Heird, Sr. Vice President, Blue Cross Blue Shield) [hereinafter "Bob Heird, Blue Cross Blue Shield, 2001 Testimony"].

189. Posting of Nancy Crino, ncrino@nricommunityservices.com, to hipaalive@lists.hipaalert.com (Sept. 25, 2001) (copy on file with Annals of Health Law).

190. Posting of William MacBain, wam@macbainandmacbain.com, to hipaalive@lists.hipaalert.com (Sept. 26, 2001) (copy on file with Annals of Health Law).

191. 45 C.F.R. § 164.504(e)(2)(ii)(A) (2000); *see also* 65 Fed. Reg. 82462, 82506 (2000); *see supra* text accompanying note 162 and 164.

agency would be prohibited from using any health information it encounters for any purposes not provided by the contract.[192] Therefore, any health information the review agency obtains while it performs a HIPAA analysis for the hospital cannot be used to create a recommendation for the health plan, even though the review agency is also a business associate of the health plan.

The examples set forth above only begin to show the administrative problems that could arise from the business associate regulations. HHS' ambiguous explanations of which individuals and organizations would be considered a business associate and the complexities involved with complying with the regulations have served only to frustrate and anger covered entities rather than protect health information. It is likely that more administrative complications will arise as each covered entity begins to identify its various business relationships and determine how health information may be disclosed or used by a business associate. It is also likely that covered entities will accordingly make demands of HHS to change the regulations.

B. Increased Litigation

Although HHS removed the third party beneficiary mandate in the business associate regulations and relaxed the duty to monitor, covered entities remain fearful of an increase in litigation by HHS and other third parties. Covered entities argue that they would still be forced to carefully monitor their business associates even though HHS removed the phrase "should have known" from the regulation.[193] Covered entities must still take reasonable steps to cure violations of the contract, which may indicate that the covered entity will have to request copies of any corrective action plan that the business associates create, periodically review how its business associates monitor such plans, and determine whether the business associates have taken steps to correct any action that would constitute a violation (i.e., if an employee leaks information to the media, it would be reasonable for the covered entity to expect that the business associ-

192. 45 C.F.R. § 164.504(e)(2)(ii)(A), (C) (2000); *see also* 65 Fed. Reg. 82462, 82505 (2000); *see supra* text accompanying note 162.

193. 65 Fed. Reg. § 82462, 82504 (200).

ate fire the employee).[194] The duty to cure, therefore, would effectively revive the proposed duty to monitor.

Business associates themselves would also face increased liability, especially if the business associate is also a covered entity. Under the regulations, members of the covered entity's workforce are not considered business associates.[195] The term "workforce" is defined as "persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."[196] HHS stated in the preamble to the final regulations that if a substantial portion of the work performed by an individual is on a covered entity's premises, the covered entity can choose whether to treat the individual as a business associates or part of the workforce.[197] HHS also stated that if no business associate agreement were in place, it would assume that the individual is a member of the workforce.[198] Despite this assumption, determining which individuals would be considered members of the workforce could have profound liability issues under the common law doctrine of ostensible agency.

For example, a physician who is an independent contractor of a hospital will either be a member of the workforce or will be considered a business associate.[199] As a member of the workforce, the hospital will be liable for any unlawful uses or disclosures of health information made by the physician (i.e., selling to Fisher Price a list of patients who recently gave birth to children). If the physician is a business associate of the hospital, his or her own liability may depend upon whether he or she is providing services "for" the hospital or "on behalf of" the hospital. A physician could provide services "for" a hospital when he or she provides regular educational seminars on the use of particular medical devices. In providing this service for the hospital, the physician would likely be held responsible for both a breach of the business associate contract and violations of HIPAA as a covered entity. If the physician, however, is provid-

194. Posting of Christine Jensen, Christine.Jensen@dhha.org, to hipaalive@lists.hipaalert.com (Oct. 18, 2001) (copy on file with Annals of Health Law).

195. 65 Fed. Reg. § 82462, 82507 (2000).

196. 45 C.F.R. § 160.103.

197. 65 Fed. Reg., 82462, 82479 (2000).

198. *Id.*

199. *See* posting of William MacBain, wmacbain@epix.net, to hipaalive@lists.hipaalert.com (May 2, 2001) (copy on file with Annals of Health Law).

ing services on behalf of the hospital, he or she may be deemed an agent of the hospital because he or she "stands in the shoes" of the hospital to perform a function on the premises of the hospital.[200] A hospital that hires a physician as a business associate to perform functions on its behalf would effectively exert some control over the physician's actions.[201] The hospital, therefore, could be found liable for the physician's violation of the privacy regulations.

An obvious solution to resolving liability issues would be to include liability provisions within the business associate contract itself. The business associate contract could state that the business associate would indemnify the covered entity or provide insurance for any violations of the business associate contract or any violations of the privacy regulations. The business associate, however, would likely limit damages to actual damages.[202] Limiting liability to an extent that would protect the business associate and still satisfy the covered entity's patients or customers may prove difficult.[203] Actual damages might not be sufficient for the person whose health information is leaked to the media, and the covered entity would likely have to make up the difference. Issues of liability could therefore be difficult to negotiate, and covered entities that also function as business associates would likely encounter these difficulties.

The AHA has suggested that a safe harbor from liability should be established for covered entities that comply with the business associate regulations.[204] It suggested that a covered entity should not be held liable to HHS for any violations that its business associates commit when it creates business associate contracts that meet all the requirements of the regulations.[205] The AHA argued that such a safe harbor would create a strong incentive for its hospitals to enter into business associate contracts.[206]

---

200. 65 Fed. Reg. 82462, 82506 (2000).

201. This example raises issues of ostensible agency theory that are beyond the scope of this paper.

202. Posting of Heather Hilliard, hhilliard@ahss.org, to hipaalive@lists.hipaalert.com (Oct. 23, 2001) (copy on file with Annals of Health Law).

203. Posting of Marcallee Jackson, marcallee@email.msn.com to hipaalive@lists.hipaalert.com (Oct. 23, 2001) (copy on file with Annals of Health Law).

204. *See* AHA Comments on Final Regulations, *supra* note 171.

205. *Id.*

206. *Id.*

Although a safe harbor provision appears to be the ideal solution to protect covered entities from excessive liability, it is not consistent with HHS' purpose of the privacy regulations. For example, Hospital has a business associate contract with Software Vendor. The business associate contract contains all the provisions that are mandated by the regulation, and accordingly would meet the safe harbor.[207] Hospital would not be liable for any unlawful uses or disclosures of its patient health information by Software Vendor. However, Software Vendor would also not be liable for the violation under the privacy regulations because it is not a covered entity. Software Vendor would only be liable for a breach of contract if Hospital decided to enforce the contract. The safe harbor provision, therefore, could effectively hold no entity liable for the unlawful use or disclosure of health information. Because HHS' purpose of the privacy regulations was to increase consumer trust in the health care system by curtailing the misuse of health information, responsibility that is consistent with this purpose needs to be placed upon the appropriate party.[208]

Although it is understandable that HHS placed responsibility of uses and disclosures upon the entities from which health information is generated, it should not create a situation in which these entities would be entirely responsible for any unlawful uses or disclosures made by their business associates. It is impossible for covered entities to effectively monitor the day-to-day activities of all their business associates and ensure that the appropriate corrective measures are in place to prevent the unlawful use or disclosure of health information. To hold covered entities liable for every possible violation of its business associates could increase the costs of providing health care and thwart the purpose of the Administrative Simplification regulations, which was to make the system more efficient and effective.

C. Action of the Covered Entities against HHS

The implementation difficulties and the possibility of increased litigation have caused covered entities to either lobby for an extension of the effective date of the regulations or challenge the authority of HHS. Some covered entities recognize the need to protect the privacy of health information, but state that they cannot comply with the regulations by the two-year

207. A review of the final regulations is found in Section III.B., notes 136-166.
208. *See generally* 64 Fed. Reg. 82462, 82470 (2000).

compliance deadline due to the inordinate costs of compliance.[209] As a result, many of these entities are asking Congress to delay the compliance deadline of the regulations.[210] For example, the National Governors Association ("NGA") has requested that Congress delay the compliance deadline.[211] The NGA estimated that the regulations would collectively cost the states an estimated $5 billion annually, which would have a severe impact on state budgets. The lack of changes to HIPAA or federal funding would also cause states to divert scarce funds to comply with the federal mandate, which translates into less money for education, capital investment, homeland security, and any efforts needed to prevent the threat of bioterrorism.[212] The states, therefore, have sound reasons for a delay of the compliance deadline.

In addition to the request for a delay, some covered entities have challenged the constitutionality of the regulations. For example, the South Carolina Medical Association ("SCMA") claimed that the privacy regulations to be unconstitutional because they were drawn up by a federal agency, as opposed to Congress.[213] SCMA also argued that § 264(c)(2), which is the provision that delegated the authority to HHS to promulgate the privacy regulations, was unconstitutionally vague.[214] Currently, the SCMA challenge is still pending. However, if successful, a lawsuit such as this could effectively eliminate the privacy regulations or greatly reduce its scope.

As if HHS sensed that it would be faced with the constitutionally challenges, it stated in the preamble to the final regulations that it has not exceeded the authority delegated to it by Con-

209. *See e.g.*, Bob Heird, Blue Cross Blue Shield, 2001 Testimony, *supra* note 188, at *10 ("Considering the multitude of relationships that [Blue Cross Blue Shield has] with other organizations, [it is] concerned that two years is insufficient time to inventory all business associate relationships and re-negotiate contracts.") ·

210. *Id.*; *see also Medical Records Privacy: Congressional Testimony before the House Committee on Energy W.J. 'Billy' Tauzin, Chairman Subcommittee on Health Hearing Assessing HIPAA*, 107th Cong. (2001) (statement of John D. Clough, Director, Health Affairs Cleveland Clinic Foundation), *at* 2001 WL 2006320, *4.

211. *Governors Continue to Support HIPAA Delay to Strengthen National Safety Net, Stimulate the Economy*, HIPAAdvisory (2001), *at* www.hipaadvisory.com/news/2001/1005nga.htm (last visited June 26, 2002).

212. *Id.*

213. South Carolina Medical Association, et al. v. U.S. Dept. of Health and Human Services, at 2, (D. S. C. filed 2001) *at* www.hipaadvisory.com/news/NewsArchives/stories/southcarolinacomplaint.pdf. (last visited June 26, 2002).

214. *Id.*

gress. HHS explained that Congress explicitly gave the agency the authority to regulate the uses and disclosures of health information that were authorized.[215] It explained that if it did not regulate the contracts with business associates, the covered entities would be able to circumvent the requirements set forth by the regulations and health information would be unprotected.[216] HHS stated that the consequential burdens placed upon the covered entities were not as important as the "very real and very significant" benefit of health care privacy.[217] HHS firmly believed that the complex regulations necessarily reflected the complex nature of the health care industry, and sought to protect the privacy of health information at each stage of transmission.[218]

It appears, however, that Congress did not intend to give HHS unfettered discretion to create the privacy regulations. Section 264 was supposed to be used by HHS as the foundation from which it would build the privacy regulations, but it never stated that HHS could extend the regulations as it saw fit. Section 264(c)(1) states that if Congress was unable to promulgate final privacy regulations by a particular date, then HHS was to "promulgate final regulations containing such standards."[219] The regulations accordingly had to "at least" address the subjects listed in Section 264(b), which were the rights of individuals with regard to health information, the procedures by which those rights can be exercised, and "the uses and disclosures of such information that should be authorized or required."[220] The words "contain" and "at least" indicate that HHS was to minimally include those subjects listed in Section 254(b).

Furthermore, the definition of "individually identifiable health information" under the Administrative Simplification provisions, and under Section 264, suggest that HHS was not limited to promulgate regulations regarding only health information maintained or used electronically.[221] Section 1171(4) defines "health information" as "any information, whether oral or recorded in any form or medium" that is created or received by a covered entity and relates to the health care of an individ-

215. 65 Fed. Reg. 82462, 82640 (2000).
216. *Id.*
217. 64 Fed. Reg. 59918, 60019 (2000).
218. 65 Fed. Reg. 82462, 82567 (2000).
219. 42 U.S.C. § 1320d-2(c)(1) (2000).
220. *Id.* at § 1320d-2(b)(3).
221. *Id.* at § 1320d-2(c)(1).

ual.[222] "Individually identifiable health information" was created as a subset of "health information" which included information kept "in any form or medium" that could reasonably be used to identify an individual.[223] Therefore, the Administrative Simplification provisions do not appear to limit the scope of the regulations to information that is kept in electronic format.

Nonetheless, Congress limited the extent to which health care activities could be regulated. Congress stated in the legislative history of HIPAA that "protecting the privacy of individuals is paramount," but it recognized that certain uses, such as referrals from a primary care physician to a specialist, were appropriate.[224] Congress implied that the privacy regulations were not to interfere in the necessary flow of information.[225] Therefore, Section 264(b) was the foundation upon which HHS could create the regulations, but the regulations could not expand to the point where they would interfere with the necessary flow of health information.

The business associate regulations appear to exceed the limitation Congress placed on HHS. The business regulations were promulgated to indirectly control how health information could be used and disclosed by third party individuals or entities, and to inform consumers about such activity.[226] Since covered entities are already bound by the regulations, they would be required to control the uses and disclosures of health information, and they would have to inform individuals about how their health information could be used or disclosed through the mandated privacy notice.[227] Accordingly, two covered entities that have a business relationship should not be required to enter into a business associate contract.[228]

---

222. *Id.* at § 1320d(4); *see also* 65 Fed. Reg. 82642, 82619 (2000).

223. 42 U.S.C. § 1320d(6).

224. H.R. Rep. No. 104-496(I), at 100 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1900.

225. *Id.*

226. *See* 64 Fed. Reg. 59918, 59948 (1999) ("If business partners of a covered entity were able to make wider use or make more disclosures than the covered entity, the patients or enrollees of the covered entity would have difficulty knowing how their information was being used and to whom it was being disclosed.")

227. *See* AHA Comments on Final Regulations, *supra* note 171 ("Covered entities. . .are already bound by the regulations with respect to any protected health information they create or receive.")

228. *Id.*

In addition, the imposition of the business associate regulations between relationships of covered entities creates "double" liability, despite the exceptions HHS created to the regulations (i.e., physician referrals and a hospital's grant of privileges do not give rise to business associate relationship).[229] Not only would a covered entity be responsible for a violation of the privacy regulations, but it could also be responsible for another covered entity's violation and responsible for a breach of contract.[230] Therefore, mandating business associate contracts among covered entities could effectively deter covered entities from entering into necessary business relationships with other covered entities, or conversely, it could create a large web of increased liability.

V. Conclusion

"[T]here is a danger that a bullet which ought to be intended for commercial and employer abuses of privacy ends up hitting medical and public health research, and damages interests that are as vital to patients as their interest in privacy."[231] Unfortunately, the business associate regulations have caused the bullet to stray, and health care providers and organizations have been injured.

Health care providers and organizations do not doubt the need for greater protections of health information. Reports of severe misuse shock the conscious of any person who is involved in health care as much as the consumers who read the reports. However, there needs to be a balance between protecting the privacy of health information and regulating the individuals and entities that handle the information. The business associate regulations do not present that balance. The regulations' requirements have created an enormous burden on the covered entities to determine which individuals and organizations would be considered business associates. At the same time, the regulations have placed virtually unlimited liability on covered entities for violations by their business associates. The business associate regulations, therefore, attempt to protect the privacy of health information to the detriment of the covered entities that must comply with them.

229. *See supra* notes 158-161 for exceptions to the business associate regulations.
230. *See supra* notes 199-201.
231. Starr, *supra* note 10, at 198.