North Dakota Law Review

Volume 73 | Number 1 Article 5

1997

Privacy of Medical Records - The Health Insurance Portability and Accountability Act of 1996 Creates a Framework for the Establishment of Security Standards and the Protection of Individually Identifiable Health Information

Francoise Gilbert

PRIVACY OF MEDICAL RECORDS? THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 CREATES A FRAMEWORK FOR THE ESTABLISHMENT OF SECURITY STANDARDS AND THE PROTECTION OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

FRANÇOISE GILBERT*

INTRODUCTION

The computerization of medical records and the increased reliance upon computers, telecommunications, and other technologies has caused patients, health care providers, and many other participants in the provision of health care to focus on patient privacy and medical record confidentiality. A question arises as to whether the new technologies increase or decrease the exposure to misuse or disclosure of information that many consider to be their most—or one of their most—important secrets. The debate will continue as society adapts to these new modes of processing information and people better understand the capabilities (good or bad) of the technology. Currently, professional organizations and private interest groups are lobbying for the enactment of laws that address this concern.

In the past, most health care issues have been under the control of each of the fifty states. These matters were considered to be local in nature. The Tenth Amendment to the United States Constitution clearly grants each state the power to legislate health care issues, including the protection of medical records privacy. As a result, a wide range of laws that attempt to preserve the confidentiality of health information currently exist. Unfortunately, since there was no concerted effort, there is no

* Françoise Gilbert, Esq.; 10 South Wacker Drive, Suite 4000, Chicago, IL 60606. Tel.: (312) 715-4984. Fax: (312) 715-4800. E-mail: fgilbert@interserv.com

Françoise Gilbert is a partner at the firm of Altheimer & Gray. Her practice focuses on high technology matters, and in particular, the use of high technology in the provision of health care. She works on contracts and policies; technology acquisitions; patient privacy protection; and contractual and tort liability prevention. She advises groups formed at both the regional and federal level on legal issues associated with telemedicine in connection with the drafting of legislation.

Ms. Gilbert teaches Information Technology Law in the graduate program of Health Care Information Systems Management at the University of Illinois, Chicago Campus. She is the Chair of the Legal and Regulatory Issues Task Force of the American Telemedicine Association; a representative of the American Bar Association to the National Conference of Lawyers and Scientists; the Secretary of the American Bar Association Science and Technology Section; and the chair of that section's Health Care Informatics Committee. Ms. Gilbert is also a member of the Board of Directors of the American Telemedicine Association.

Ms. Gilbert holds law degrees from Loyola University's Chicago School of Law and Paris University School of Law (France) and undergraduate and graduate degrees in Mathematics from Paris University and Montpellier University (France). She is licensed to practice law in both Illinois and France.

uniformity in the protection, or lack thereof, provided by these statutes. Meanwhile, the attempts at creating uniform legislation have failed. To date, the Uniform Health Care Information Act, which was completed in 1985, has been enacted only by two states: Montana,[1] in 1987, and Washington,[2] in 1991.

The development of health care networks, and the availability of long distance health care through telemedicine, have added a new dimension to the concern for protection of individual health care information. In the traditional setting, patients, providers, and payers were all located in the same state. Consequently, health care issues were naturally a matter of state concern. Today, however, it is increasingly common that tests or X-rays of a patient who is residing in one state be transmitted, by courier or electronically, to another state to be read and interpreted. Full-fledged consultations can also be conducted long distance through the techniques of telemedicine. For a specialist in a remote city to be able to assess a patient's medical condition, the complete medical records of the patient may have to be sent via modem or satellite between the state where the patient resides and the state where the specialist is practicing. When several physicians in different states participate concurrently in the provision of care to a single patient and when that patient's medical information crosses state borders, it can be argued that the provision of health care becomes an interstate commerce issue and thus a federal, rather than a state matter.

There have been many attempts in the past several years to enact federal legislation that addresses the protection of health information privacy. To date, these efforts have failed. Five medical records privacy bills were introduced in the 104th Congress: Senate Bill 7, Senate Bill 872, Senate Bill 1360, House Resolution 435, and House Resolution 3482. Several of these bills were discussed in committees, but none of them were enacted into legislation. As of February 10, 1997, only House Resolution 435 has been reintroduced before the 105th Congress. It is now House Resolution 52 and is designated as the *Fair Health Information Practices Act of 1997.* It can be expected that this and other bills will continue to be discussed during the 105th Congress. Since the

1. MONT. CODE ANN. § 50-16-501 (1995) (stating Montana enacted the Uniform Health Care Information Act in 1987). Montana has adopted the entire Uniform Health Care Information Act. *See* MONT. CODE ANN. §§ 50-16-501 to -553.

2. WASH. REV. CODE ANN. § 70.02.005 (West 1992) (stating Washington enacted the Uniform Health Care Laws in 1991). The State of Washington has adopted the entire Uniform Health Care Information Act. *See* WASH. REV. CODE ANN. §§ 70.02.005 - .904 (West 1992 & Supp. 1993).

concept of protection of confidentiality of medical records appears to have the attention of both parties, the chances to see legislation enacted by this Congress might be higher.[3]

In the meantime, the Health Insurance Portability and Accountability Act of 1996 (Portability Act) was enacted on August 21, 1996. The new Act lists as its numerous purposes:

> to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, and to simplify the administration of health and insurance.[4]

The Portability Act is divided into five titles. Title I amends the Employee Retirement Income Security Act of 1974 (ERISA) and the Public Health Service Act by adding provisions with respect to health plan portability, availability, and renewability of health insurance coverage. Title III, which amends the Internal Revenue Code of 1986, focuses on medical savings accounts, deductions for health insurance costs, and the treatment of long-term care services. Title IV provides for the application and enforcement of group health plan requirements, while Title V focuses on revenue offsets.

Title II of the Portability Act addresses the prevention of health care fraud and abuse, and requires simplification of the administration of health claims. Subtitle F of Title II focuses on "administrative simplification" by creating standards for communications.[5] Its goal is to "improve the Medicare Program . . ., the medicaid program . . ., and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[6] Section 262 of the Portability Act focuses on the enactment of standards for the electronic transmission of health information and addresses the need to protect security, integrity, and authenticity of health information. To date, § 262 appears to be the piece of legislation that is the most able to provide some guidance and relief in framing an adequate protection for health care information.

3. Senate Bill 1360, introduced in the 104th Congress, was a bipartisan bill. The bill received much attention from the press and in Congress, and there were high hopes that it would mature into legislation.

4. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 1996 U.S.C.C.A.N. (110 Stat.) 1936.

5. 42 U.S.C.A. § 1320d to d-8, 1395cc, 242k (Supp. IVA 1996).

6. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 261, 1996 U.S.C.C.A.N. (110 Stat.) 1936, 2021 (codified in scattered sections of 42 U.S.C.A.).

This article reviews the provisions of § 262 of the Portability Act. The analysis is structured as follows:

I. EFFECT ON STATE LAW

Title II, Subtitle F of the Portability Act requires the establishment of standards and requirements to facilitate the electronic transmission of certain health information.[7] Section 262 of the Portability Act amends Title XI, and is codified in 42 U.S.C.A. § 1301 *et seq.* The provisions of Subtitle F are meant to supersede any contrary provisions in state law. Section 262 of the Portability Act provides that standard or implementation specifications adopted under § 262 of the Portability Act "shall supersede any contrary provision of state law . . . that requires

7. Health Insurance Portability and Accountability Act § 261.

medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form."[8]

There are limits to the mandate. A provision or requirement for a standard or implementation specification set forth in Subtitle F of the Portability Act cannot supersede a contrary provision of state law if the provision of State law is "necessary - (I) to prevent fraud and abuse; (II) to ensure appropriate state regulation of insurance and health plans; (III) for State reporting on health care delivery or costs; (IV) for other purposes; or . . . . addresses controlled substances; or . . . relates to the privacy of individually identifiable health information."[9] Other exceptions are carved out for public health and state regulatory reporting requirements.[10]

II. DEFINITIONS

A. STANDARDS

Standards are defined as "any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1320d-1 through 1320d-3 of this title."[11] The standards must "enable health information to be exchanged electronically."[12]

There are only limited guidelines about the nature of the standards: the standards must be enacted to reduce "the administrative costs of providing and paying for health care;"[13] and a standard may "not require disclosure of trade secrets or confidential commercial information by a person required to comply" with the statute.[14] In addition, § 262 of the Portability Act requires the adoption of the following:

- universal identifiers for each participant, i.e., individuals, employers, health plans and health providers;[15]

8. 42 U.S.C.A. § 1320d-7.

9. *Id.* § 1320d-7(2).

10. The provisions of § 1320d-7(a) cannot "be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention." *Id.* § 1320d-7(b). They also cannot be interpreted to "limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification." *Id.* § 1320d-7(c).

11. *Id.* § 1320d(7).

12. *Id.* § 1320d-2(a)(1).

13. *Id.* § 1320d-1(b).

14. *Id.* § 1320d-1(e).

15. *Id.* § 1320d-2(b).

- security standards or safeguards to ensure the integrity and confidentiality of the information and protect against threats to security or integrity of the information and unauthorized uses of the information;[16] and
- standards for the authentication of electronic signatures.[17]

There are no other general requirements with respect to the type of standards, their nature, their scope, how they would be defined, or what they would cover.

B. HEALTH INFORMATION

The standards to be created under § 262 of the Portability Act apply generally to the transmission of health information. "Health information" is defined as:

> any information, whether oral or recorded in any form or medium, that -
>
> (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
>
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[18]

This definition of health information is very similar to that which has been used in other legislation or pending bills with respect to the protection of patients' medical records. For instance, the new House Resolution 52 (an updated version of House Resolution 435, which was introduced in the 104th Congress) uses almost the same definition.

16. *Id.* § 1320d-2(d).
17. *Id.* § 1320d-2(e)(1).
18. *Id.* § 1320d(6).

III. SCOPE

A. TO WHOM AND TO WHICH INSTITUTIONS THE STANDARDS WILL APPLY

The standards adopted under Title II, Subtitle F of the Portability Act will apply to health plans,[19] health care clearinghouses,[20] and health care providers[21] who transmit any health information in electronic form in connection with certain financial or administrative transactions.[22] The provisions of § 262 of the Portability Act do not apply, however, to financial institutions that are covered by the Right to Financial Privacy Act of 1978, or entities that are "engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, . . . with respect to such activities."[23]

19. *Id.* § 1320d-1(a). A "health plan" is "an individual or group plan that provides, or pays the cost of, medical care." *Id.* § 1320d(5). Under the definition, "health plan" includes the following, or a combination thereof:

(A) A group health plan . . . but only if the plan - (i) has 50 or more participants as defined in § 1027(7) of Title 29); or (ii) is administered by an entity other than the employer who established and maintains the plan.
(B) A health insurance (as defined in § 300gg-91(b) of this title).
(C) A health maintenance organization (as defined in §300gg-91(b) of this title).
(D) Part A or B of the medicare program under subchapter XVIII of this chapter.
(E) The medicaid program under subchapter XIX of this chapter.
(F) A medicare supplemental policy (as defined in § 1395ss(g)(1) of this title).
(G) A long-term care policy, including a nursing home fixed indemnity policy . . .
(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purposes of offering or providing health benefits to the employees of 2 or more employers.
(I) The health care program for active military personnel under Title 10.
(J) The veterans health care program under chapter 17 of Title 38.
(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of Title 10.
(L) The Indian health service program under the Indian Health care Improvement Act (25 U.S.C. § 1601 et seq.).
(M) The Federal Employees Health Benefit Plan under chapter 89 of Title 5.

Id. § 1320d(5).

20. *Id.* § 1320d-1(a). A "health care clearing house" is "a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." *Id.* § 1320d(2).

21. *Id.* § 1320d-1(a). "Health care providers" include "a provider of services[,] . . . a provider of medical or other health services, and any other person furnishing health care services or supplies." *Id.* § 1320d(3).

22. *Id.* § 1320d-1(a).

23. *Id.* § 1320d-8. Examples of transactions or activities that are not subject to the requirements of the Portability Act include:

(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.
(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1) - (A) for transferring receivables; (B) for

B. TO WHICH TRANSACTIONS THE STANDARDS WILL APPLY

Only certain types of transactions must comply with the standards requirements. These are transactions "with respect to:

(A) Health claims or equivalent encounter information.
(B) Health claims attachments.
(C) Enrollment and disenrollment in a health plan.
(D) Eligibility for a health plan.
(E) Health care payment and remittance advice.
(F) Health plan premium payments.
(G) First report of injury.
(H) Health claim status.
(I) Referral certification and authorization."[24]

Even though the creation of standards in these limited areas will inevitably facilitate other aspects of health care management, important components are left unaddressed. For example, health care information is also used for internal quality control, for utilization review, to assist in risk management programs, for management of institutional resources, to determine credentials, as part of the peer review process to assess the quality or appropriateness of care, for licensure and accreditation of health care institutions, and to report deaths, births and communicable diseases. Most of these uses are not specifically addressed, even though some of them, such as accreditation or peer review, are essential to the provision of high quality health care and require access to health information. It remains to be seen whether the standards listed above will be sufficient to permit attempts to organize in a concerted manner all data necessary for the performance of the activities listed above. Creating standards for the management and transmission of these data would add efficiency to the monitoring and certification processes, reduce the administrative burden, and thereby save money to all parties.

IV. THE DIFFERENT TYPES OF STANDARDS

Section 262 of the Portability Act focuses on a limited number of standards. These include a standard for the identification of the parties to the transactions (individuals, employers, health care providers, and payers); security standards to ensure the integrity and confidentiality of the

auditing; (C) in connection with - (i) a customer dispute; or (ii) an inquiry from, or to, a customer; (D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer; (E) for reporting to consumer reporting agencies; or (F) for complying with - (i) a civil or criminal subpoena; or (ii) a Federal or State law regulating the entity.

Id.

24. *Id.* § 1320d-2(a)(2).

information; standards specifying procedures for the electronic transmission and authentication of signatures; and standards for the transfer of information among health plans.[25]

A. UNIQUE HEALTH IDENTIFIERS

Section 262 of the Portability Act requires the use of a "unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system."[26] Though such a rule makes sense because it simplifies the administrative process, it causes great concern with respect to the protection of confidentiality because it makes it easier to compile databases of information about individual patients. The Portability Act recognizes that there may be a need to set limits on the way a single identifier is used. It is provided that standards adopted under 42 U.S.C. § 1320d-2(b)(1) "shall specify the purposes for which a unique health identifier may be used."[27] There is no mention, however, of the types of limitations and restrictions on the uses of a unique health identifier, nor is there mention of the contrary, obligations to use them.

The use of unique health identifiers has often been discussed in the past. Many are concerned that associating each individual with a unique health identifier would create yet another link to a person, making it easier to add information to compilations of personal data at a time when commercial databases contain an already huge amount of private information about each of us. Unfortunately, it is probably already too late. Typically, a person's social security number has been used as an alternative to a specific universal identifier, whether in health related matters or other circumstances. Nowadays, one is very frequently required to provide a social security number in many commercial transactions, such as banking, car rentals, and many health care procedures. If a unique health identifier different from the social security number were created, it is inevitable that databases would quickly establish the connection between the two sets of personal identifiers.

On the other hand, requiring the use of a different personal identifier for each type of procedure would make it almost impossible to manage information for those who need to do so. For example, it would cause many problems in a hospital's record management system, where patients need different types of procedures on a regular basis over a long period. However, one practical alternative might be a combination of a public universal identifier with a private personal identification number

25. *Id.* § 1320d-2.
26. *Id.* § 1320d-2(b)(1).
27. *Id.* § 1320d-2(b)(2).

that would be under the control of each person or patient, and that the individual would, or could, change at will. Another alternative would be a system of keys similar to those used when sending and receiving encrypted messages, where an individual has a public key (i.e., non-secret) and a private key (i.e., secret), with the private key being neccessary to unlock the protected information.

B. SECURITY AND SAFEGUARDS

Title II, Subtitle F of the Portability Act acknowledges that security, integrity, authenticity, and confidentiality of information must be maintained. Although the provisions are somewhat limited, they set the stage for a better protection of the confidentiality of health care information. Health plans, health care clearinghouses, and health care providers that maintain or transmit health information are required to maintain:

> reasonable and appropriate administrative, technical and physical safeguards:
>
> (A) to ensure the integrity and confidentiality of the information;
>
> (B) to protect against reasonably anticipated -
>
> (i) threats or hazards to the security or integrity of the information; and
>
> (ii) unauthorized uses or disclosures of the information; and
>
> (C) . . . to ensure compliance . . . by [their respective] officers and employees.[28]

In addition, health care clearinghouses that are part of a larger organization are required to have policies and security procedures that "isolate the activities of the health care clearinghouse with respect to processing information in a [way] that prevents unauthorized access to such information by the larger organization."[29]

One shortcoming of this section is that it does not define what "confidentiality" means, that is, it fails to explain who can or cannot have access to specific information.[30] Therefore, the current uncertainty with respect to the scope of confidentiality requirements (i.e., who has access to what) is not yet resolved. However, by imposing upon health plans and health care providers a requirement that they implement such structures, the Portability Act provides a technical setting for better discipline and awareness in the management of health information.

28. *Id.* § 1320d-2(d)(2).
29. *Id.* § 1320d-2(d)(1)(B).
30. *Id.*

C. GUIDELINES FOR THE SECURITY STANDARDS

Section 262 of the Portability Act does not provide specific criteria for security standards, but only requires the Secretary of Health and Human Services (Secretary) to adopt security standards that take into account:

(i) the technical capabilities of record systems used to maintain health information;
(ii) the costs of security measures;
(iii) the need for training persons who have access to health information;
(iv) the value of audit trails in computerized record systems; and
(v) the needs and capabilities of small health care providers and rural health care providers.[31]

Great freedom is left to the standard setting organizations. It might have been useful to provide specific guidelines or requirements on the nature of the security standards to be implemented by each health plan or health care provider. By failing to do so, the time it will take to implement these guidelines and requirements will be increased.

D. AUTHENTICATION

Section 262 of the Portability Act also addresses the concern for authentication of the messages sent by requiring the adoption of standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions.[32] The ability to sign documents electronically has been the source of great concerns in the past because many states had laws, commonly known as "Quill Pen Laws," which required that medical records be signed in ink, thereby preventing the use of electronic records. By acknowledging the ability to use electronic signatures, the Portability Act allows the elimination of an antiquated requirement, which will greatly and rapidly contribute to the universal adoption of electronic medical records.

E. STANDARDS FOR THE TRANSFER OF INFORMATION AMONG HEALTH PLANS

Finally, the Portability Act requires the enactment of standards for the transfer of information among health plans.[33] There is no specific

31. *Id.* § 1320d-2(a)(1).
32. *Id.* § 1320d-2(e)(1).
33. *Id.* § 1320d-2(f).

direction as to what these standards are supposed to achieve. The only directive is that the Secretary must "adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan."[34]

V. REQUIREMENTS FOR TRANSACTIONS MADE BY HEALTH PLANS

Health plans that wish to conduct financial or administrative transactions are required to comply with the standards.[35] There are at least three circumstances where those transmitting health information must comply with the requirements.[36] The Act provides that if a person wishes to conduct a transaction with a health plan as a standard transaction:

> (A) the health plan may not refuse to conduct such transaction as a standard transaction;
> (B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction or the ground that the transaction is a standard transaction; and
> (C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.[37]

There is no excuse for failing to comply, and no exception to compliance with this rule. Compliance may be achieved, either directly by "transmitting and receiving standard data elements of health information,"[38] or indirectly, by "submitting nonstandard data elements to a health care clearinghouse for processing into standard data elements and transmission by the health care clearinghouse, and receiving standard data elements through the health care clearinghouse."[39]

34. *Id.*
35. *Id.* § 1320d-4(a)(1).
36. *Id.*
37. *Id.*
38. *Id.* § 1320d-4(a)(2)(A).
39. *Id.*

VI. PENALTIES FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

A. GENERAL PENALTY

The Secretary is allowed to "impose on any person who violates a provision . . . a penalty of not more than $100 for each such violation." There is a cap of $25,000 on the penalty that may be imposed for all violations of an identical requirement or prohibition during a calendar year.[40]

Defenses may be used in the case of the threat of assessment of a penalty: by claiming the non-compliance was not discovered, or by claiming the failure to comply was due to a reasonable cause. Indeed, § 262 of the Portability Act provides that a penalty may not be imposed if it is established that "the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision."[41]

Another defense is that the failure to comply was due to reasonable cause, not to willful neglect, and the failure to comply was corrected within thirty days after the person liable for a penalty knew, or by exercising reasonable diligence would that known, that the failure to comply occurred.[42] The thirty-day period may be extended based on the nature and extent of the failure to comply, and the Secretary may provide technical assistance as she deems appropriate.[43] The penalty may also be waived if the payment of such penalty would be excessive relative to the compliance failure involved.[44]

B. WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Greater penalties are assessed in the case of wrongful disclosure of individually identifiable health information. "Individually identifiable health information" is defined as:

> any information, including demographic information collected from an individual, that -
> (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of

40. *Id.* § 1320d-4(a)(2)(B).
41. *Id.* § 1320d-5(b)(2).
42. *Id.* § 1320d-5(3)(A).
43. *Id.* § 1320d-5(3)(B).
44. *Id.* § 1320d-5(4).

> health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and -
> (i) identifies the individual; or
> (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[45]

A more substantial penalty than in the case of inadvertent non-compliance is assessed against one who knowingly, and in violation of the law: "(1) uses or causes to be used a unique health identifier; or (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person."[46]

In the case of a knowing violation, the offender may:

> (1) be fined not more that $50,000, imprisoned not more than one year or both;
> (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than five years, or both; and
> (3) if the offense is committed with intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than ten years, or both.[47]

This provision is crucial to the protection of the confidentiality of medical records. Indeed, there is a pervasive use of compiled health information for marketing purposes, which constitutes a serious invasion of a person's privacy, and against which it has been difficult to fight because appropriate legislation was missing. For example, a network of drugstores may have gathered information about the customers who have purchased prescription drugs at different stores over the years. These databases may contain a name, address, telephone number, social security number, credit card number, a list of the drugs acquired by each patient, and hence a description of each patient's health profile. It is then possible to process the data to extract lists of patients with a specific condition. In fact, recently a case was reported where a person who had

45. *Id.* § 1320d(6).
46. *Id.* § 1320d-6(a).
47. *Id.* § 1320d-6(b). Unlike the clause which provides a penalty in case of an inadvertent violation, this provision does not define the penalty according to the number of violations, but states only a maximum dollar amount or a maximum number of years. *Id.* This inconsistency in drafting may cause interpretation problems.

a miscarriage began receiving advertisements for diaper services at about the time the baby should have been born had the pregnancy reached its normal term. One wonders who had the information about the pregnancy and how the information made it into the mailing list of the diaper service. This new law might help reduce the abuses of database owners who make commercial uses of personal health information.

VII. CREATION AND IMPLEMENTATION OF THE STANDARDS

A. WHO CREATES THE STANDARDS

The Portability Act contemplates that the standards will be created by standard setting organizations,[48] unless they are promulgated by the Secretary, who may do so if another standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives.[49]

B. TIMETABLE

1. For Enactment

The timetable for the development of the standards is relatively short. The Secretary has eighteen months from the enactment of the Portability Act to enact the standards described above, except for the standards relating to claims attachments, for which the time frame is increased to thirty months.[50] Thereafter, the standards may be modified, but not more frequently than once every twelve months.[51]

2. For Compliance

For initial standards, any person to whom the standard applies must comply with the standard or specification within twenty-four months after the date on which an initial standard or implementation specification is adopted or established.[52] However, in the case of small health plans, the initial implementation period is increased to thirty-six

48. "Standard setting organizations [are the] standard setting organization[s] accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation [of the Portability Act]." *Id.* § 1320d(8).

The Portability Act also requires that specific organizations be consulted: the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Interchange, and the American Dental Association. *Id.* § 1320d-1(c)(3). Groups such as AHIMA, AMIA, and AMA, surprisingly, are not included in the list. It seems odd that these groups were left out; perhaps it was an oversight on the part of Congress.

49. *Id.* § 1320d-1(c)(3)(ii).

50. *Id.* § 1320d-3(a).

51. *Id.* § 1320d-3(b)(1).

52. *Id.* § 1320d-4(b)(1)(A).

months.[53] What constitutes a "small health plan" is not defined, but the Portability Act requires the Secretary to determine which plans qualify as "small health plans."[54] If a standard is modified, the Secretary will have to specify the period within which compliance must be achieved, but such period may not be shorter than 180 days after the date of adoption of the modification.[55]

CONCLUSION

By providing for the creation of standards for the transmission of electronic health information and requiring the implementation of security and confidentiality procedures, the Health Insurance Portability and Accountability Act is major progress in the development of an efficient and secure computerized health information management system. The Act sets forth the framework for bringing medical record management and processing into the twenty-first century. It acknowledges the existence of computers and electronic data processing, and imposes structures and safeguards to better take advantage of the technology while attempting to limit the detrimental effects on human beings. The Act has set a demanding calendar for the enactment of these standards. Much remains to be done when developing clear and simple regulations to implement this legislation, and when developing the standards themselves.

The Act, however, does not address with sufficient specificity the issue of confidentiality. Although it provides the means to protect confidentiality and integrity of individual health information, it does not deal with the different shades of "confidentiality," that is, what is to be kept strictly confidential, who can or cannot have access to which information, and the limits to secondary uses of health information. It remains clear that more specific legislation addressing in general the confidentiality of individual health information is needed to define the respective rights and obligations of the increasing number of players in the distribution of health care services.

53. *Id.* § 1320d-4(b)(1)(B).
54. *Id.*
55. *Id.* § 1320d-4(b)(2).