Privacy of Medical Records:

IT Implications of HIPAA

David Baumer, Ph.D., J.D.; Julia Brande Earp, Ph.D.; Fay Cobb Payton, Ph.D.
Department of Business Management,
North Carolina State University
David_Baumer, julia_earp, fay_payton@ncsu.edu

Abstract: Increasingly, medical records are being stored in computer databases that allow for efficiencies in providing treatment and in the processing of clinical and financial services. Computerization of medical records has also diminished patient privacy and, in particular, has increased the potential for misuse, especially in the form of nonconsensual secondary use of personally identifiable records. Organizations that store and use medical records have had to establish security measures, prompted partially by an inconsistent patchwork of legal standards that vary from state to state. There is widespread appreciation among policy makers regarding the need for legal reform. The Health Information and Portability Accountability Act of 1996 mandated that the Administration develop regulations regarding the control of medical records. The Administration has offered regulations from the Department of Health and Human Services (Standards for Privacy of Individually Identifiable Health Information; Proposed Rule 45 CFR Parts 160 through 164). Survey data reveal what healthcare professionals who have access to sensitive medical records believe are the greatest threats to patients' privacy. The overlap between Administration proposals and the responses of healthcare professionals is striking.

I. Introduction

Passage of the Health Insurance and Portability Accountability Act (HIPAA) in 1996 required the Clinton Administration, via the Office of Health and Human Services (HHS), to compose uniform standards for electronic exchanges of health information if Congress failed to enact a comprehensive privacy act by August 21,1999. 1When Congress failed to act by the August 1999 deadline, HHS responded with proposed regulations on November 3, 1999.2 We examine the regulations offered by the Department of Health and Human Services (HHS) (Standards for Privacy of Individually Identifiable Health Information; Proposed Rule 45 CFR Parts 160 through 164), which became law, February 21, 2000.3 These regulations, however, do not preempt current state laws that provide greater protection for the privacy of medical records.4

As might be expected, there are numerous controversies on both sides of the privacy debate. Some think that the protections contained in the proposed records are inadequate, while others contend that privacy safeguards will erode the efficiencies that computerized medical records create, impede medical research and, in some cases, interfere with law enforcement.5 We (Drs. Earp and Payton) conducted a survey of healthcare workers at a healthcare provider whose employees have access to personally identifying medical records.6 The healthcare provider, whose employees are the respondents for the survey, will be regulated under the HHS Rule discussed in this paper. We compare the Administration's proposed regulations (the HHS Rule) with the survey responses of those who have access to medical records. There is a strong correlation between what healthcare workers regard as objectionable and what is outlawed by the proposed HHS Rule.

II. Background of the Privacy Debate Regarding the Privacy of Individually Identifiable Medical Records

A. Current Federal Protection for the Privacy of Medical Records

Legal protection for the privacy of medical records is a crazy patchwork that is in desperate need of reform.7 To date there is no federal statute that protects the bulk of personally identifiable medical records. The Americans with Disabilities Act (ADA) and the Privacy Act of 1974 provide some protection under some circumstances.8 Also for government employees, the Fourth Amendment requires a showing of probable cause when their employer (the government) searches

their medical records. For the vast bulk of medical records, however, there is currently little or no effective legal protection for the privacy of individually identifiable medical information at the federal level.9 When medical records are not protected a number of abuses can and do take place including:

* unauthorized secondary use of medical records,
* inaccuracies that are not corrected,
* discovery and disclosure of medical records by hackers and commercial vendors,
* use of medical records by employers for employment decisions, and
* revelation of medical records by employees of insurance companies, who may be among our neighbors and who do not have medical training.

The Privacy Act of 1974 provides some protection for medical records that are held by federal agencies, but does not cover medical records held by private groups where most of the medical records are created and stored.10 Likewise, the Privacy Act has numerous exceptions so that its protection is leaky at best. In its time, the Privacy Act was heralded as a huge step forward, but currently it has been labeled as the "most outdated" privacy act in the world. 11

Some protection for medical records is also contained in the American with Disabilities Act (ADA) of 1990, which outlaws discrimination based on disabilities. As long as a disabled person can perform the essential functions of the job, employers cannot refuse to hire an applicant based on disability and must make reasonable accommodations for them to perform the job functions. The protection for medical records of employees under ADA is also filled with loopholes. First, the ADA does not protect the medical records of those who are not defined under the Act as "disabled." If the employee is considered "disabled", according to one of the three criteria detailed in the ADA, disclosure of medical records is permitted when:

(1) the supervisor needs to be informed regarding the necessary restrictions on the duties of the employee,

(2) when the employer's medical staff needs to be informed for purposes of emergency treatment, and

(3) when government officials seeking to determine compliance with the ADA.12

A recent case illustrates the vulnerability of employees who are considered disabled under the ADA. In Doe v. SEPTA a self-insured, public employer hired Pierce to audit medications taken by employees to determine if waste and fraud were taking place.13 Doe was infected with the AIDS virus and was reluctant to apply for benefits under the company plan because he feared detection. Doe specifically asked company officials whether Pierce would have access to his records and was told by the company that there was no need for Pierce to match Doe's name with the treatment he was receiving. Nevertheless, Pierce did match Doe's name up with his prescriptions and soon Doe's supervisor and coworkers learned of his condition. Doe sued under 42 § U.S.C. 1983 for deprivation of his constitutional right to privacy, but after winning at the District Court level, Doe lost a Court of Appeals decision, which held that the greater good outweighed Doe's privacy concerns. Pierce had saved SEPTA more than $42,000,000 in medical and dental bills, and the court indicated that the benefits of Pierce's actions, "outweighs the minimal intrusion into Doe's privacy." 14

B. Privacy Protection at the State Level

Much of the legal protection for the privacy of medical records occurs at the state level. Unfortunately, there is no uniformity across state jurisdictions so that compliance with state statutes by those creating, storing and using medical records is difficult given the wide disparities in protection. To add to the confusion, plaintiffs in medical disclosure cases must rely on state common law claims that are riddled with anomalies and exceptions. In 30 of the 50 states invasion of privacy by the unreasonable publicity given to the private facts of a person's life is actionable.15 Attempts to fashion uniform state laws regarding medical records have been a spectacular failure. To date, only two states have adopted the Uniform Healthcare Information Act (UHCIA).16 The UHCIA itself only applies to healthcare providers and does not apply to third parties such as insurers and claims processors. The National Association of Insurance Commissioners (NAIC) has endorsed the Health Information Privacy Model Act, but this bill does not apply to healthcare providers.17

C. Impact of Technology

The debate regarding the privacy of medical records has been sharpened by several long-term trends. First, there is intense pressure to contain costs of medical treatment, not only among Medicare patients, but also by private insurers and employer health plans. There is increased scrutiny by third-party payers of medical treatments, tests and all kinds of psychiatric care. HMOs are caught in middle between the demands of patients for appropriate medical treatment and the costs they can recover from private and public insurers. Computerization of medical records can yield significant savings, but with it comes increased opportunities for disturbing disclosures. Second, much of the current privacy protection is based on paper records, which are being replaced by computerized files. The laws that were adequate for paper records are often inadequate to provide protection for computerized records. Computerized medical records are much more amenable to abuse on a much larger scale. Additionally, the exposure to detection of snoopy employees and others with access to medical files is much less when operating through a computer, than when they have to access paper records stored in visible file cabinets. The impacts of security breaches of company protocols that inadequately protect stored records are much more significant

than with paper records. Third, as technology progresses, the potential for more intrusions into personal medical records will grow, particularly in the area of DNA testing. The potential use of DNA test results by insurers and employers to exclude "undesirables" from risk pools is becoming more and more evident.18

D. Need for Reform

There is general recognition that legal protection for the privacy of medical records is inadequate and disorganized. The debate about the privacy of medical records pits, privacy advocates and patients, against insurers, healthcare providers, public health organizations, researchers, law enforcement, government agencies, educational institutions and many others. Not surprisingly, each special interest has a rationale as to why it deserves access to personally identifiable medical records without obtaining consent of patients.

In some cases, personally identifiable medical records are sold to commercial interests (often at large profits) for direct marketing campaigns. Given the large amounts of revenue at stake, health organizations that are often labeled, "pro-patient" are enticed to traffic in sales of such information.19

E. Fair Information Principles

The basic building blocks of federal confidentiality law are not in dispute. In the Geocities case, the Federal Trade Commission prosecuted a business that maintained a website that collected information from website visitors.20 Following the Geocities decision, the FTC issued a report, which stated its views on fair information principles.21 According to the FTC privacy report, there are generally accepted fair information principles that all websites (and repositories for medical information) should subscribe to:

(1) Notice/Awareness-consumers (patients) should be notified as to who is gathering the data and the uses that will be made of that data.

(2) Choice/Consent-consumers (patients) should consent to any secondary use for the data. There should be opt-in and opt-out provisions.

(3) Access/Participation-consumers (patients) should have the right to contest the accuracy of the data collected.

(4) Integrity/Security-there should be managerial mechanisms in place to guard against loss, unauthorized access, or disclosures of the data.

(5) Enforcement/Redress-there should be remedies available to victims of information misuse. The FTC envisions self-regulation by industry groups, private rights of action based on invasion of privacy, and government enforcement as in the Geocities case.

There is, however, considerable debate as to how to translate these principles into practice. Healthcare advocates of privacy question the need for circulation of individually identifiable data beyond that necessary for healthcare providers and treatment. Others involved in the healthcare sector favor exceptions for various reasons. Among the exceptions are: facilitation of approvals and third-party payment systems, medical research, and desires of public healthcare associations. Hospitals, insurers, claims agents, managed care organizations, health researchers and law enforcement view the sharing of healthcare information as essential to the efficient functioning of the healthcare system.22 These groups desire uniform federal laws that are understandable and which eliminate obstacles, including consent of the patients, to the sharing of healthcare information.

III. Department of Health and Human Services: Standards for Privacy of Individually Identifiable Health Information; Proposed Rule

In an effort to deal comprehensively with the issue of privacy of medical records, HHS developed a proposed Rule that occupied 145 pages of the Federal Register on November 3, 1999.

A. Making the Case for Additional Privacy Standards

According to the HHS proposed regulations, under the title Need for Privacy Standards,

> The maintenance and exchange of individually identifiable health information is an integral component of the delivery of quality healthcare. In order to receive accurate and reliable diagnosis and treatment patients must provide healthcare professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. Healthcare providers, health plans and healthcare clearinghouses also rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to received needed care, the quality of that care, and the efficiency with which it is delivered."23

The foregoing statement by HHS recognizes (1) that effective medical care requires transfer of medical (and other) information from patient to healthcare professionals and (2) that other health organizations have legitimate needs to access healthcare information to facilitate payments and enhance treatment. According to the HHS, "Efforts to provide legal protection against the inappropriate use of individually identifiable health information has been, to date, undertaken primarily by the States."24 Further, HHS states that, "The number of entities maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years...[t]he expanded use of electronic information has had clear benefits for patients and the healthcare system as a whole."25 Finally, according to HHS, "The absence of national standards for the confidentiality of health information has, however, made the healthcare industry and the population in general uncomfortable about this prima-

rily financially driven expansion in the use of electronic data."26

B. Statutory Background

According to HHS regulations, "section 262 [of HIPAA] directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, healthcare clearinghouses, and healthcare providers who transmit electronically in connection with such transactions."27 Also the regulations recite Section 264(c)(1) of the HIPAA which provides that:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1171(a) of the Social Security Act (as added by section 262) is not enacted by (August 22, 1999), the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than (February 21, 2000).28

Since Congress did not enact such legislation, HHS is required to act. Among the goals of the proposed HHS standards are:

* Allow for the smooth flow of identifiable health information for treatment, payment and related operations, and for purposes related to healthcare that are in the public interest.
* Prohibit the flow of identifiable information for any additional purposes, unless specifically and voluntarily authorized by the subject of the information.
* Put into place a set of fair information practices that allow individuals to know who is using their health information and how it is being used.
* Establish fair information practices that allow individuals to obtain access to their records and request amendment of inaccurate information.
* Require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure.
* Hold those who use individually identifiable health information accountable for their handling of this information, and to provide legal recourse to persons harmed by misuse.29

Clearly, these goals have much in common with the report by the Federal Trade Commission that discusses Fair Information Principles following the GeoCities action.

C. Limitations and Protections Contained in HHS Proposed Regulations

Although the report of HHS recommends that, "'everyone in this chain of information handling be covered by the same rules.' HIPAA limits HHS authority to covered entities, which include health plans, healthcare clearinghouses and any healthcare provider who transmits health information in electronic form..."30 "In particular, the proposed regulation does not directly cover many of the persons who obtain identifiable health information from the covered entities."31 HHS, however, attempts to expand their authority by requiring those receiving health records to apply the same fair information principles as the covered entities. Those receiving protected healthcare information from a covered entity may be classified as "business partners."

The basic thrust of the HHS Rule is to prohibit covered entities from using or disclosing protected health information except as provided in the proposed rule. Covered entities could use or disclose protected health information without authorization (from the patient) for treatment, payment and healthcare operations.32 Covered entities would be allowed to disclose healthcare information without authorization only in very narrowly specified public health and public policy-related purposes, "including public health, research, health oversight, law enforcement..." According to HHS, "A central aspect of this proposal is the principle of 'minimum necessary' disclosure."33

D. Permissible Uses and Disclosures for Purposes Other Than Treatment, Payment and Heath Care Operations

Although the proposed HHS rule adheres to a 'minimum necessary' disclosure principle, it does elucidate a long list of exceptions to the requirement to obtain individual authorization before disclosure of medical records. Most of these exceptions are based on public policy considerations, but the terms are potentially very elastic. Much of the controversy involves the details of the exceptions to the general principles of privacy that require individual authorization for secondary use of medical information. HHS considered permitting only those disclosures required by law, but decided that these exceptions are so important to public health and other purposes, that some unauthorized secondary disclosures should be permitted.34 Although the sale of medical records for commercial purposes is not included among the exceptions, secondary use of the information might, and probably will, take place. The following sections describe some of the exceptions for disclosure without individual authorization.

1. Public Health Activities

The HHS Rule proposes to allow disclosure of medical records without individual authorization by covered entities for purposes of, "carrying out public health activities authorized by law, to non-governmental entities authorized by law to carry out public health activities, and to persons who may be at risk of contracting or spreading a disease (when other law authorizes notification)."35 The (HSS) Rule goes on to note that the covered entity could also be a public health agency and the same rules would apply. The Rule indicates that traditional public health activity to combat the spread of communicable diseases is so important that individual inter-

ests in privacy are overridden by community interests. If the HHS rule interfered with the transmission of such information, it would require major changes in the ordinary practices of public health officials and would potentially expose people to communicable diseases.

2. Disclosure for Health Oversight Purposes

Chief among health oversight purposes are, "combating fraud in the healthcare industry, ensuring nondiscrimination, and improving quality of care..." according to the HHS Rule.36 According to HHS, "[O]versight activities are a national priority in part because of the losses in the healthcare system due to error and abuse..." which the HHS Office of Inspector General estimates at about 7 percent.37 The Rule indicates that much of the work can be done with statistical tests that do not require disclosure of individual records without authorization, not all of the oversight activities can be carried in that manner.

3. Use for Judicial and Administrative Proceedings and for Use by Coroners and Medical Examiners

The HHS Rule envisions disclosures in personal injury and medical malpractice cases, "in which the medical condition of a person is at issue..." and a judicial or administrative proceeding is taking place to determine the cause of the injury or medical condition.38 The HHS Rule indicates these disclosures, "are clearly necessary to allow the smooth functioning of the legal system."39 In addition, the HHS rule would allow disclosure of medical records to coroners and medical examiners.40 Again, public interest in determining causes of death is cited as well as the disclosure requirement by state law.

4. Disclosures to Law Enforcement

The HHS Rule would permit unauthorized secondary disclosure of individually identifiable medical records if the request by law enforcement is pursuant to judicial or administrative process. In addition, disclosure of medical information to law enforcement could occur without a search warrant if the disclosures by covered entities were given in good faith for fraud detection or to reveal a criminal action. The disclosure of healthcare information under this exception would generally be pursuant to a search warrant, absent exigent circumstances.41 HHS admits that it has not figured out all of the boundaries of appropriate releases to law enforcement.

5. Government Health Data Systems and Health Directories

HHS proposes to allow secondary use of protected health information without individual authorization if the disclosure is, "authorized by State or other law to support policy, planning, regulatory, or management functions."42 According to HHS governmental (including federal) examination of individually identifiable health data plays an essential role in examining the effectiveness of various policies. Moreover, if such transfers of information were prohibited, then HIPAA would negatively impact ongoing procedures that are routinely used by governments to evaluate policies that require detailed information that can only be obtained by examining protected health information. Unless the patient objects, the HHS Rule proposes to allow a health facility to include patients in a directory. For those patients who are not disabled at the time, the HHS Rule would require the facility to obtain information from the patient. The patient could specify to the health facility who would be entitled to receive the protected health information and who would not be so entitled.

6. Disclosure for Banking and Payment Purposes

According to the HHS Rule, checks and credit card payments of necessity will disclose protected health information.43 The HHS contends that, "Failure to allow this kind of disclosure of protected health information would impede the efficient operations of the healthcare system."44 Recognizing what is likely to become commonplace in the future, the Rule states that, "We understand that financial institutions may also provide covered entities that accept payment via credit card with software that, in addition to fields for information to process the transaction, includes blank fields in which health plans or healthcare providers may enter any type of information regarding their patients, such as diagnostic and treatment information, or other information that the covered entity wished to track and analyze."45 Going further, the HHS Rule suggests that banks could become, "business partners of covered entities in accordance with and subject to the conditions of § 164.506(e)."46 By becoming business partners of a covered entity, banks would become subject to the same prohibitions regarding protected health information as the covered entities.

7. Medical Research

HHS permits covered entities to disclose (to entities pursuing medical research) protected medical information without authorization as long as, "the covered entity receives documentation that the research protocol has been reviewed by an Institutional Review Board or equivalent body-a privacy board-and that the board found that the research protocol meets specified criteria (regarding protected health information) designed to protect the subject."47 In the absence of such documentation, medical researchers would have to obtain permission from the individuals who supplied the information, i.e., the patient. HHS stresses the importance of medical research that has led to many breakthroughs that have had dramatic impacts on the nation's health.

E. Concluding Thoughts about the Proposed HHS Rule

The absolutist wing of privacy lobby would limit secondary use of individually identifiable to situations in which indi-

vidual authorization has been obtained. On the other hand, at present, there is no overall protection for the privacy of privately held medical information that is individually identifiable. The Administration's approach, through the HHS Rule, is to split the difference between nearly a complete absence of protection and prohibitions on distribution of medical information for purposes other than treatment (the absolutist approach). Reasonable people can disagree about whether the proposed HHS Rule achieves its objective of "the minimum disclosure required".

The Administration's regulations would allow for unauthorized disclosure of medical information, not only for treatment, but also for payment and healthcare operations. The second goal of the Administration's Rule is to require individual authorization for secondary uses of medical information that is individually identifiable. The HHS Rule, however, allows for a lengthy list of exceptions to the requirement for individual authorization for secondary use of the protected medical information. Most of these exceptions reflect commercial practices within the healthcare industry currently extant. Most of the exceptions are justified on public policy grounds from prevention of the spread of communicable diseases, to detection of fraud, facilitating the justice system, and medical research where obtaining permission adds significantly to costs.

IV. Views of Healthcare Workers Who Have Access to Medical Records

A recent survey by Earp and Payton reveals the concerns of healthcare workers regarding the privacy of medical records.48 In order to be eligible to take the survey, the respondent had to be a healthcare worker who had access to patient records. The survey was administered to a diverse group of 163 respondents (133 females, 30 males, 114 whites, 40 African-Americans, 9 Hispanics) who have extensive experience in healthcare (average number of years in healthcare 10.6, average age 44.6, and average number of years with current employer 5.2).

A. Frequency Data

The survey data consist of the responses of healthcare workers to statements made about healthcare issues involving privacy, access to, uses made of, and the accuracy of medical records. The survey instrument and response data are available in the Appendix as well as some descriptive statistics. The responses varied from 1 to 7, with 1 indicating strong disagreement with the statement and 7 indicating strong agreement.

B. Gathering Patient Information

In Table 1 of the Appendix, survey data are arranged according to weighted-average responses to the statements in the questionnaire, from lowest to highest. Statements E, A, and O all relate to requests by their employer to gather information from patients. There are three variations of the same statement, which is, "I am troubled by requests from my employer to gather information from patients." The response data clearly indicate that healthcare workers are not troubled by the gathering of information from patients. Part of this lack of concern could, of course, be motivated by self-interest since knowledge by healthcare workers of any communicable diseases will enable them to take preventive measures. In addition, more knowledge of medical and other conditions of the patents enables healthcare workers presumably to better evaluate and treat patients.

C. Accuracy of Records

Statement G essentially says that their employer should never use information given by patients for any other reason than medical treatment. The average response of 4.28 indicates that healthcare workers were undecided about that statement. The word, "never" seems too strong in this context. Responses to statements H, B, L, and F all concern the accuracy of the files containing medical records. Some variations of the statement suggest that their employer should devote more time and resources to making sure that the records are accurate. The response data indicate that healthcare workers recognize that the accuracy of medical files is a problem and that more resources should be devoted to enhancing the accuracy of these records.

D. Access to Records

Statements N, I and D refer to access to patient records by others, not including the patient. Survey responses indicate that healthcare workers are very cognizant about possible abuses in the form of unauthorized or inappropriate access to medical records that contain personal information. Healthcare workers appear very concerned about the inappropriate and unauthorized access to medical records that is made possible by computerized medical records maintained by their employer. Note that it is much less obvious for a healthcare worker or others to invade the privacy of computerized medical records than for the same person to rummage through paper records in file cabinets. On a scale that varies between 1 and 7, the average response across statements N, I, and D was 5.94 agreeing with the statement that unauthorized and inappropriate access to personal medical records is a serious problem.

E. Unauthorized Secondary Use

Statements C, M, and K all refer to unauthorized secondary access and use of personal medical records. Again, using the same scale, the average response was 6.36 condemning unauthorized secondary use of patient information. Probably the greatest source of resentment among patients is that vendors in the medical sector will somehow access their medical records and that they will be targeted for marketing cam-

paigns based on what is in their medical files. Note that the highest agreement among healthcare professionals with access to medical records is for the statement that their employer, "should never sell the patient information in its computer databases to other companies."

F. Implications of Analysis of Frequency Data

Based on the frequency data it seems fair to say that:

* Healthcare professionals do not regard the gathering of patient information as an abuse or source of concern.
* Healthcare workers recognize that information received from patients may sometimes be required for purposes other than treatment.
* There are significant concerns among healthcare workers about the accuracy of medical files and that employers should do more to improve accuracy of medical records.
* There are also very significant concerns among healthcare workers about inappropriate and unauthorized access to medical records.
* Healthcare workers take most seriously unauthorized secondary use of medical information. The most egregious abuse, in the view of healthcare workers, occurs when a company sells computerized medical files for money.

G. Factor Analysis

A factor analysis reveals much the same results. Based on the factor loadings the following four variables were created (in order of significance): Errors (concern about the accuracy of patient medical records), Unauthorized Secondary Use, Improper Access, and Collection (of data).

V. Conclusion

Most major advances in technology also entail unintended consequences. As computerized medical records have enabled healthcare providers to efficiently gather and evaluate medical information, via modern database and database-enabled technologies, the potential for misuse of this information has also increased. Among the major players in the health sector are insurers, employers, hospitals, pharmaceutical companies, healthcare researchers, public health administrators, vendors of medical equipment, various levels of government, medical researchers, law enforcement, and of course, healthcare providers. Each of these players has there own rationale as to why they are entitled to individually identifiable medical records. In most cases, the rationale put forward by these groups are well-thought out, but the combined impact is one that leaves patients feeling exposed as too many people are seeing patients' medical records.

The principles of fair use of information have been agreed upon for at least 25 years. Implementation, however, has been contentious because various groups argue that there should be exceptions. The most fundamental principle of fair use of information is that no secondary use of medical information should take place unless authorized by the patient. The HHS Rule, promulgated by the Clinton Administration, allows numerous exceptions to this principle based on public health policy considerations, commercial practices, and state laws. Although the proposed regulations of HHS allow for exceptions to the principles of fair use of information, they still represent a major step forward in protecting medical records.

Healthcare workers are on the frontlines of the privacy battle. They know that the gathering of information is essential effective treatment and for processing claims. Healthcare workers also know that these medical records are not always accurate and that too many have access to these records. Finally, healthcare workers know there is something inherently wrong about unauthorized secondary use of medical information that does not involve treatment, payment, or operations and that the sale of medical information without authorization should be prohibited. ◆

Notes:

1 42 U.S.C.A. 1320d to d-8 (West Supp. 1998).
2 Federal Register 59918 et seq., Dept. of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 through 164, Standards for Privacy of Individually Identifiable Health Information, (November 3, 1999), (hereinafter Fed. Reg.)
3 Fed. Reg. 59921.
4 Fed. Reg. 59926. The essence of the proposed federal Rule is that it would provide a floor for the privacy of medical records. The Rule is not intended to replace state common law or statutory laws affecting privacy.
5 Bartley L. Barefoot, Enacting a Heath Information Confidentiality Law: Can Congress Beat the Deadline?, 77 N.C.L. Rev. 283 (1998).
6 Earp and Payton, Information Privacy Concerns Facing Healthcare Organizations in the New Millennium, under review at the Journal of American Medical Information Association.
7 Barefoot, 1998..
8 42 U.S.C. 12112 (1994); 5 U.S.C. 552a (1994).
9 HHS notes that, "Efforts to provide legal protection against the inappropriate use of individually identifiable health information have been, to date, undertaken primarily by the States." Fed. Reg. 59919-20.
10 5 U.S.C. 552a (1994).
11 Barefoot, 294.
12 42 U.S.C. § 12112(c)(3)(B).
13 73 F.3d 1133 (3rd Cir. 1995).
14 Id., at 1143.
15 Causes of action in the other 20 states for disclosure of medical records are unknown to the authors. Twomey, LABOR AND EMPLOYMENT LAW, 584. In 22 states patients do not have the right to view their own medical records, CNN Broadcast of Congressional Hearings regarding HHS Rule, February 17, 2000.
16 Barefoot 304.
17 Id., 305.
18 Mark A. Rothstein, Betsy D. Gelb, and Steven G. Craig, Protecting Genetic Privacy by Permitting Employer Access Only to Job-Related Employee Medical Information: Analysis of a Unique Minnesota Law, 24 Am. J. L. and Med. 399 (1998).
19 Barefoot 288.
20 Geocities; Analysis to Aid Public Comment,Thursday, August 20, 1998, 63 Federal Register
44624 AGENCY: Federal Trade Commission
21 www.ftc.gov/reports/privacy3/index.htm.
22 Barefoot 309.

23 HSS Regs, I.A. The Need for Privacy Standards, Fed. Reg. 59919.
24 Fed. Reg. 59919-20
25 Fed. Reg. 59920.
26 Id.
27 Id.
28 Fed. Reg. 59921.
29 Fed. Reg. 59923.
30 Fed. Reg. 59923-4.
31 Id.
32 Fed. Reg. 59924.
33 Fed. Reg. 59943.
34 Fed. Reg. 59955.
35 Fed. Reg. 59956.
36 Fed. Reg. 59957.
37 Id.
38 Fed. Reg. 59958.
39 Fed. Reg. 59959.
40 Fed. Reg. 59960.
41 Fed. Reg. 59961.
42 Fed. Reg. 59964.
43 Fed. Reg. 59966.
44 Fed. Reg. 59966.
45 Id.
46 Id.
47 Fed. Reg. 59967.
48 Julie Earp and Fay Cobb Payton, Information Privacy Concerns Facing Healthcare Organizations in the New Millennium, Working Paper, NCSU, College of Management.

Table 1: Frequency Data for Survey

	SD						SA		
	1	2	3	4	5	6	7	Wtd Sum	Wtd Avg
E. XXXX should devote more time and effort to preventing unauthorized access to patients' personal and financial information.	48	25	16	39	20	7	1	451	2.89
A. It usually bothers me when XXXX asks patients for their personal and financial information.	35	39	12	45	16	3	6	469	3
O. XXXX should take steps to make sure that unauthorized persons cannot access patient information in its computers.	38	22	14	64	10	4	4	482	3.09
G. XXXX should take more steps to make sure that the patient information in its files is accurate.	19	17	22	30	15	17	36	668	4.28
H. When patients give personal information to XXXX for some reason, XXXX should never use the information for any reason (other than its original intent).	2	5	9	52	25	22	41	791	5.07
J. Computer databases that contain patient information should be protected from unauthorized access - no matter how much it costs.	2	4	10	44	27	27	41	807	5.17
D. XXXX should not use patient information for any purpose unless it has been authorized by the patient who provided the information.	3	4	8	42	23	26	50	824	5.28
B. It usually bothers me when XXXX asks patients for their personal and financial information.	5	7	8	22	31	41	42	826	5.29
L. XXXX should never sell the patient information in its computer databases to other companies.	2	3	2	32	41	35	41	844	5.41
F. When XXXX asks patients for personal and financial information, I sometimes think twice before recording it.	4	3	7	26	30	33	53	854	5.47
C. All the patient information in computer databases should be double-checked for accuracy - no matter how much this costs.	5	6	7	10	11	20	97	932	5.97
I. XXXX should have better procedures to correct errors in patient information.	2	3	2	11	22	37	79	943	6.04
M. XXXX should devote more time and effort to verifying the accuracy of the patient information in its databases.	3	1	1	5	8	23	115	1011	6.48
N. XXXX should never share patient information with other companies unless it has been authorized by the patients who provided the information.	2	1	1	5	9	21	117	1017	6.51