

ISSUE BRIEF

Protecting the Confidentiality of Health Information

Friday, September 18, 1998
Washington, DC

A roundtable discussion featuring

Don Detmer, M.D.

University Professor of Health Policy
University of Virginia
Chair
National Committee on
Vital and Health Statistics

with commentary from

Jerry Avorn, M.D.

Chief
Division of Pharmacoepidemiology
and Pharmacoeconomics
Brigham and Women's Hospital
Boston

A. G. Breitenstein

Director
JRI Health Law Institute
Boston

Deborah Hammond, M.D.

Vice President, Medical Management
Systems Support
Prudential HealthCare
Roseland, New Jersey

Chris Koyanagi

Director of Legislative Policy
Bazelon Center for
Mental Health Law
Washington, DC

Harriet Pearson

Director of Public Affairs
IBM Corporation

Joy Johnson Wilson

Director, Health Committee
National Conference on
State Legislatures
Washington, DC

Protecting the Confidentiality of Health Information

As the use of information technology spreads, concerns about the confidentiality of health information increase. The public has become aware that much personal information is widely available and beyond the control of the individual. Medical records, which often contain personal and sensitive information, seem particularly vulnerable. In today's health care marketplace, a multitude of entities—managed care companies, retail pharmacies, employers, and researchers—may have access to personally identifiable health information.

Many policymakers have taken note of these concerns and have called for federal legislation to protect the confidentiality of health information, yet consensus on how best to craft legislation remains elusive. Certain to be contentious and complex, federal legislation would affect numerous stakeholders. Many consumer and physician groups argue that proposed legislation does not go far enough to maintain the trust between physicians and patients, thereby jeopardizing the quality of care delivered. Moreover, some consumer groups are concerned about how health information is currently being used beyond the realm of health care (for example, for law enforcement activities or employment decisions). Therefore, they call for strict limits on its use. At the same time, those who use health information to deliver, finance, research, track, and evaluate health care-related services worry that legislation will impede their ability to share information and, therefore, make less information available for important health-related evaluation (such as outcomes analysis, performance measurement, research, and public health activities). Indeed, these users of information believe there is a major disconnect between demands for greater accountability in the health care system and demands for privacy rights.

The Forum recently distributed a comprehensive background paper on the confidentiality of health information, prepared by Lise Rybowski. This Forum session will concentrate on three of the key issue areas raised in that paper: controlling access to health information, conducting research, and preempting state laws.

THE IMPETUS FOR LEGISLATION

A combination of factors has led to the call for a legislative solution to protect the confidentiality of

health information. The most obvious stimulus is the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which effectively set a deadline for Congress to act to protect personal privacy. HIPAA required the secretary of health and human services to make recommendations to Congress, in consultation with the National Committee on Vital and Health Statistics (NCVHS), on ways to protect individually identifiable information and to establish penalties for wrongful disclosure of personal health information. The secretary presented those recommendations in September 1997; Congress now has until August 1999 to enact a privacy law. If Congress fails to act, the secretary is directed to promulgate regulations within 42 months of HIPAA enactment (by February 21, 2000) relating to the privacy of health information transmitted in connection with specified electronic transactions.

HIPAA also contains administrative simplification requirements designed to facilitate standardized, electronic transmission of certain administrative and financial health-related transactions. In fact, the privacy provisions were included in HIPAA due to concerns about the administrative simplification provisions.

DHHS is now in the process of issuing a series of proposed regulations related to administrative simplification standards. Since May, the department has released regulations relating to a uniform electronic health care

ISSUE BRIEF/No. 724

Analyst/Writer

Nora Super Jones

National Health Policy Forum

2021 K Street, NW, Suite 800
Washington, DC 20052

202/872-1390

202/862-9837 (fax)

nhpf@gwu.edu (e-mail)

www.nhpf.org (Web site)

Judith Miller Jones, Director

Karen Matherlee, Co-Director

Sandra M. Foote, Co-Director

Michele Black, Publications Director

NHPF is a nonpartisan education and information exchange for federal health policymakers.

claim (and other common administrative transactions), unique identifier numbers for health care providers and employers, and security standards for electronic health data. In releasing the security regulations on August 11, Secretary of Health and Human Services Donna Shalala said that, while the standards are crucial, they are “not enough.”¹ In addition, she called for new legal protections to safeguard the privacy of medical records in *all* forms.

One administrative simplification standard that has yet to be released has generated tremendous controversy and drawn sharp criticism from medical and privacy advocates.² Under HIPAA, DHHS is required to adopt a unique health identifier number for each American. The Clinton administration has said no proposal for patient identifier numbers will be implemented until privacy protections have been put in place. According to DHHS officials, the timetable and substantive requirements of HIPAA envisioned that federal privacy protections would be in place at the same time the transactions standards, standard identifiers, and system security measures were implemented. If Congress fails to enact a privacy law by August 1999, HIPAA requires DHHS to issue regulations to protect the confidentiality of information transmitted in connection with the standardized transactions described in the law. These regulations would have to be finalized by February 2000, before the effective date of the uniform data standards.

Other factors that increase pressure for legislative action include:

- The notable progress of information technologies over the last several years and the corresponding increase in the usefulness and ubiquity of health care data.
- Growing awareness of the use of personal medical data by various health care corporations for commercial advantage.
- The growth of managed care, which has greatly increased the number of entities that have access to personal health information and, in turn, has accentuated concerns about privacy among both clinicians and patients, particularly with respect to ways that information may be used to create barriers to care and coverage.
- International pressures centered around a European Union directive, effective October 1998, that prohibits member nations from disseminating information to organizations outside the country that do not provide an adequate degree of privacy protection.

PENDING LEGISLATION

In response, Congress has stepped up its efforts to enact privacy legislation. All of the major patient protection bills pending in Congress contain confidentiality provisions. All would give individuals the right to inspect and copy their medical records, except in special circumstances. For example, a Senate GOP bill (S. 2330), a bill introduced by Sen. Edward M. Kennedy (D-Mass.) and Rep. John D. Dingell (D-Mich.) (S. 1890/H.R.3605), and one sponsored by Sen. John H. Chafee (R-R.I.) (S. 2416) contain broad requirements for plan-associated health professionals and facilities to post their confidentiality practices and to establish appropriate safeguards to protect the confidentiality of individually identifiable information. The bills do not define these practices and safeguards.

The House Republican-crafted Patient Protection Act of 1998 (H.R. 4250) contains more detailed provisions relating to medical records confidentiality. Under the bill, “any person who maintains protected health information may disclose the information to a health care provider or a health plan for the purpose of permitting the provider or plan to conduct several health care operations.” Health care “operations” are defined as

services, provided directly by or on behalf of a health plan or health care provider or by its agent, for any of the following purposes: (a) Coordinating health care, including health care management of the individual through risk assessment, case management, and disease management. (b) Conducting quality assessment and improvement activities, including outcomes evaluation, clinical guideline development and improvement, and health promotion. (c) Carrying out utilization review activities, including precertification and preauthorization of services, and health plan rating activities, including underwriting and experience rating. (d) Conducting or arranging for auditing services.

Critics have charged that the term “health care operations” is so broad it could apply to anything, including the transfer of patient information to companies marketing new drugs.³ Moreover, privacy advocates want the confidentiality provisions to be considered separately from the broader patient protection bill. Health care industry representatives disagree, stating that the House-passed bill achieves a balance between consumers’ concerns over the confidentiality of health information and their demands for high quality, affordable health care services.⁴

While the fate of this broad legislation remains uncertain, several proposals focused exclusively on

medical records confidentiality are circulating in Congress. Sens. James M. Jeffords (R-Vt.) and Christopher T. Dodd (D-Conn.) have introduced the *Health Care Personal Information Nondisclosure Act of 1998* (S. 1921); and Sens. Patrick J. Leahy (D-Vt.) and Kennedy have put forward the *Medical Information Privacy and Security Act* (S. 1368); Sen. Robert F. Bennett (R-Utah), who sponsored legislation during the last session of Congress, is also drafting a bill that is expected to be introduced this fall.

In the House, Reps. Christopher R. Shays (R-Conn.) and Thomas M. Barrett (D-Wis.) have introduced the *Consumer Protection and Medical Record Confidentiality Act of 1998* (H.R. 3900), Rep. Jim McDermott (D-Wash.) has introduced the *Medical Privacy in the Age of New Technologies Act of 1997* (H.R. 1815), and Rep. Gary A. Condit (D-Calif.) sponsored the *Fair Health Information Practices Act of 1997* (H.R. 52).

The differences in the bills highlight some of the most contentious issues:

- What are the appropriate uses of personally identifiable information? To what extent can personally identifiable information be disclosed without patient authorization? For what purposes and under what conditions?
- Should federal regulations be applied to both federally and nonfederally funded researchers that use personally identifiable data?
- How broad should federal preemption of state laws pertaining to confidentiality be?

Consent

All of the bills pending in the House and the Senate would require, as a general rule, patient consent prior to disclosure. The bills then set forth specific situations and conditions, which vary from bill to bill, under which information could be disclosed without consent. The standards for disclosure for law enforcement activities, in particular, vary widely.

Most bills would establish a two-tiered authorization process. That is, they would allow health care entities to require individuals to provide a first level of authorization for certain uses of personal health information as a condition to receiving care or providing payment.⁵ After this requirement had been met, a second level of authorization would be required for disclosures not related to treatment or payment, and individuals would be permitted to refuse to consent to disclosures without suffering adverse consequences.

For instance, the Jeffords bill would require that employers, health plans, and, under certain circumstances, providers obtain a single authorization to disclose an individual's protected health information for purposes of treatment, payment, and health care operations.⁶ A separate authorization would be required for other purposes, including "for disclosure with intent to sell, transfer, or use protected health information for commercial advantage." The Shays bill would not require a first-level authorization for treatment, payment, and certain health care operations. In contrast, the Leahy bill would generally prohibit the disclosure of protected health information without first obtaining an individual's authorization, except in limited circumstances. It would apply to each release of medical information including re-releases. Furthermore, the Leahy bill would allow patients to pay for treatment themselves in order to avoid disclosure of personal health information.

Research

The bills differ in their treatment of federally and privately funded research and in their reliance on the current Institutional Review Board (IRB) system. The Leahy, Condit, and McDermott bills would require approval by IRB for federally funded and nonfederally funded research. Consistent with current federal regulations, the bills would permit the IRB to waive the informed consent requirement if the potential benefit of research outweighed the privacy interest of the individual. The Shays bill would permit disclosure to health researchers if the disclosure were "reviewed by a committee, board, or informal organization in accordance with confidentiality standards specifying permissible and impermissible uses of the information."

The Jeffords bill would permit protected health information to be disclosed to a health researcher who obtains the data under the following circumstances:

- (1) from federally funded projects or institutions that have assurances on file with the Office of Protection of Human Subjects at the National Institutes of Health in compliance with rules specified by the federal government; (2) in conformance with rules promulgated by the Food and Drug Administration for new product trials; or (3) if the research is privately funded human subject research.

The bill notes that there are currently no specific procedures in place for the third classification of research. The bill would provide for the Senate Committee on Labor and Human Resources to await the recommendations of the secretary of health and human

services, after reviewing the commissioned General Accounting Office study on confidentiality and the National Bioethics Advisory Commission's report, to determine appropriate confidentiality procedures for privately funded human subject research.

Federal Preemption

The bills generally differ on whether or not to establish a floor or ceiling for federal standards. The Jeffords, Condit, and Shays bills generally would preempt most state laws except those pertaining to mental health and public health activities. The Leahy and McDermott bills would not preempt any state laws that provide a greater level of protection for personally identifiable health information. The latter position is generally consistent with the recommendations presented to Congress by DHHS.

THE FORUM SESSION

The Forum session will focus on the key issues raised by the background paper and provide an opportunity for the various stakeholders to discuss the policy implications of the options currently under consideration. In the interest of keeping the discussion focused, particular emphasis will be placed on the three topics identified earlier: controlling access to health information, conducting research, and preempting state laws.

Don Detmer, M.D., university professor of health policy at the University of Virginia, will provide an overview of the issues that must be resolved and some of the options available to legislators, regulators, and the health care industry. As chairman of the Secretary's National Committee on Vital and Health Statistics, Dr. Detmer has been closely involved in providing guidance to DHHS regarding privacy and administrative simplification requirements. As a researcher and physician, he can also provide insight into how health information is currently used. Dr. Detmer also maintains a surgical practice, co-directs the Virginia Health Policy Center, and serves as chairman of the Board of Health Care Services of the Institute of Medicine of the National Academy of Sciences and of the board of *Vhita*, a company committed to personal computer-based records.

Because of the large number of stakeholders involved in this issue and the desire to provide an opportunity for a variety of perspectives to be heard, following Dr. Detmer's comments, the session will be conducted as a roundtable discussion with several knowl-

edgeable participants at the table. Key issues and questions will be discussed by invited commentators as well as by participants in the Forum's audience. Invited discussants include the following:

Jerry Avorn, M.D., an associate professor of medicine at Harvard Medical School and chief of the division of pharmacoepidemiology and pharmaco-economics at Brigham and Women's Hospital in Boston, will discuss the research community's concerns as they relate to data privacy, including the use of IRBs and the distinction between personally identifiable and nonidentifiable data for research purposes. An internist, geriatrician, and pharmacoepidemiologist, Dr. Avorn has focused his research efforts on medication use, with particular reference to elderly patients and chronic disease. Dr. Avorn currently serves as president of the International Society for Pharmacoepidemiology.

A.G. Breitenstein, director of the Justice Resource Institute's Health Law Institute in Boston, will discuss the need to improve patient confidentiality and medical privacy. As an attorney, Ms. Breitenstein provides direct legal representation to individuals infected with HIV and youth at high risk for becoming HIV infected. She has been working on confidentiality issues for the past three years and most recently was asked to testify before Congress and NCVHS about various legislative proposals now pending. She serves as a resource to several national and state organizations, including the National Resource Council and the Massachusetts Medical Society, as they develop policy regarding the confidentiality of medical records.

Deborah Hammond, M.D., vice president of medical management systems support for Prudential HealthCare (PHC), will discuss insurance management issues and how proposed legislation might affect the plan's ability to conduct utilization review, measure the performance of providers, or otherwise do business. In addition, she will discuss the company's current practices regarding the confidentiality of health information and demands for this information from outside parties and how Prudential responds to these requests. Dr. Hammond is a physician leader in PHC, where she has served in a variety of capacities since 1986. Her current areas of responsibility include oversight of utilization management, quality improvement, pharmacy services, data capture and data warehousing, information delivery, and provider connectivity as well as interfacing with other system support areas, claims/encounter processing, provider network support, member service support, and sales and marketing.

Chris Koyanagi, legislative policy director for the Bazelon Center for Mental Health Law, will discuss the concerns of the mental health community. With over 25 years of experience as a government affairs specialist, Ms. Koyanagi has a substantial understanding of both mental health policy and the federal policy process. In her role as director of the legislative agenda for the Bazelon Center, a legal advocacy organization concerned about the rights of persons with severe mental illness, she supervises federal government relations and state initiative staff.

Harriet Pearson, director of public affairs for IBM Corporation, will discuss the perspective of large, self-insured employers. She will address how employers use health information and what safeguards are in place to protect against discrimination. Ms. Pearson directs IBM's involvement in the areas of privacy, health care, workplace policy, and environmental and energy public policy. Since 1997, she has led IBM's work on privacy policy issues, focusing particularly on Internet privacy and medical records issues

Joy Johnson Wilson, federal affairs counsel and director of the Health Committee at the National Conference of State Legislatures (NCSL), will discuss state laws in the area of medical records confidentiality and the implications of federal preemption. NCSL represents the legislatures of the 50 states, its commonwealths, territories, and the District of Columbia; its Health Committee guides the development of the organization's policy on all health care issues. As director, Ms. Wilson, who has been with NCSL since 1978, follows health care reform at both the state and federal levels, including privacy, Medicaid, and other health initiatives of importance to state legislatures.

KEY QUESTIONS

Controlling Access to Health Information

- Who should have access to individually identifiable information?
- How much access should they have? For what purposes?
- Who should control that access and how?
- Should employers (including self-insured employers) have special limits placed on their access? If so, what are the implications for their ability to make coverage decisions or ensure accountability and efficiency?

- What are common applications of personal health information? Of these, what should be permitted or prohibited?
- Under what circumstances should authorization from the patient be required for disclosures of personal health information? Should there be stricter requirements for certain types of information, for example, mental health records?
- What are the implications of requiring individual authorizations for information disclosure?
- What is the value of informed consent?
- What role should individuals have in determining who can see their information?
- Should consent be obtained from individuals to transfer personal health information to other entities, such as retail pharmacies?
- How prevalent is the sale, transfer, or use of personally identifiable health information for commercial advantage?

Conducting Research

- What activities should be defined as "research"? For example, clinical trials, outcomes research, disease management?
- How can a federal privacy law create incentives for researchers to use health data that are not personally identifiable?
- In what instances are personally identifiable data necessary to conduct research?
- If researchers were required to obtain informed consent from research subjects, what would be the implications?
- How well does the current IRB process work to protect privacy?
- Should regulations be applied to both federally and nonfederally funded researchers? That is, should IRB approval be required prior to receiving identifiable information?

Preempting State Laws

- Should federal legislation set a floor of minimum standards for privacy protection, which individual states could exceed, or should it establish a ceiling of uniform standards that must be met by all parties but can not be exceeded by the states?

-
- What are the implications of a federal “floor” approach for national health plans, pharmaceutical companies, and big hospital systems that operate across state laws?
 - Under a broad federal preemption, what would be the implications for states with stricter requirements on the books?
 - Should certain state laws, such as mental health laws, be exempt from preemption? If so, what are the implications of isolating mental health information from an individual’s medical record?

ENDNOTES

1. Department of Health and Human Services, “HHS Proposes Security Standards for Electronic Health Data,” DHHS news release, August 11, 1998. Available at <http://aspe.os.dhhs.gov/admsimp/nprm/press3.htm>, August 21, 1998.
2. Robert O’Harrow, Jr., “White House to Delay Health ID Plan on Privacy Concerns,” *Washington Post*, July 30, 1998, A2.
3. Sheryl Gay Stolberg, “Privacy Concerns Delay Medical ID’s,” *New York Times*, August 1, 1998.
4. John Schwartz, “Bill Would Allow Sale of Patient Data: Health Care Firms Could Make Disclosures,” *Washington Post*, July 24, 1998, F1.
5. Discussion of the differences between pending legislative proposals draws from the testimony of Janlori Goldman, director, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University Medical Center, before the House Committee on Government Reform and Oversight, Subcommittee on Government Management, Information, and Technology, May 19, 1998.
6. The definition of “health care operations” contained in the Jeffords/Dodd bill does not include the coordination of care or comprehensive health care management of the individual including risk assessment, prevention intervention, case management, disease system management, continuous quality research and improvement initiatives, development of best case clinical guidelines, and other essential health care services.