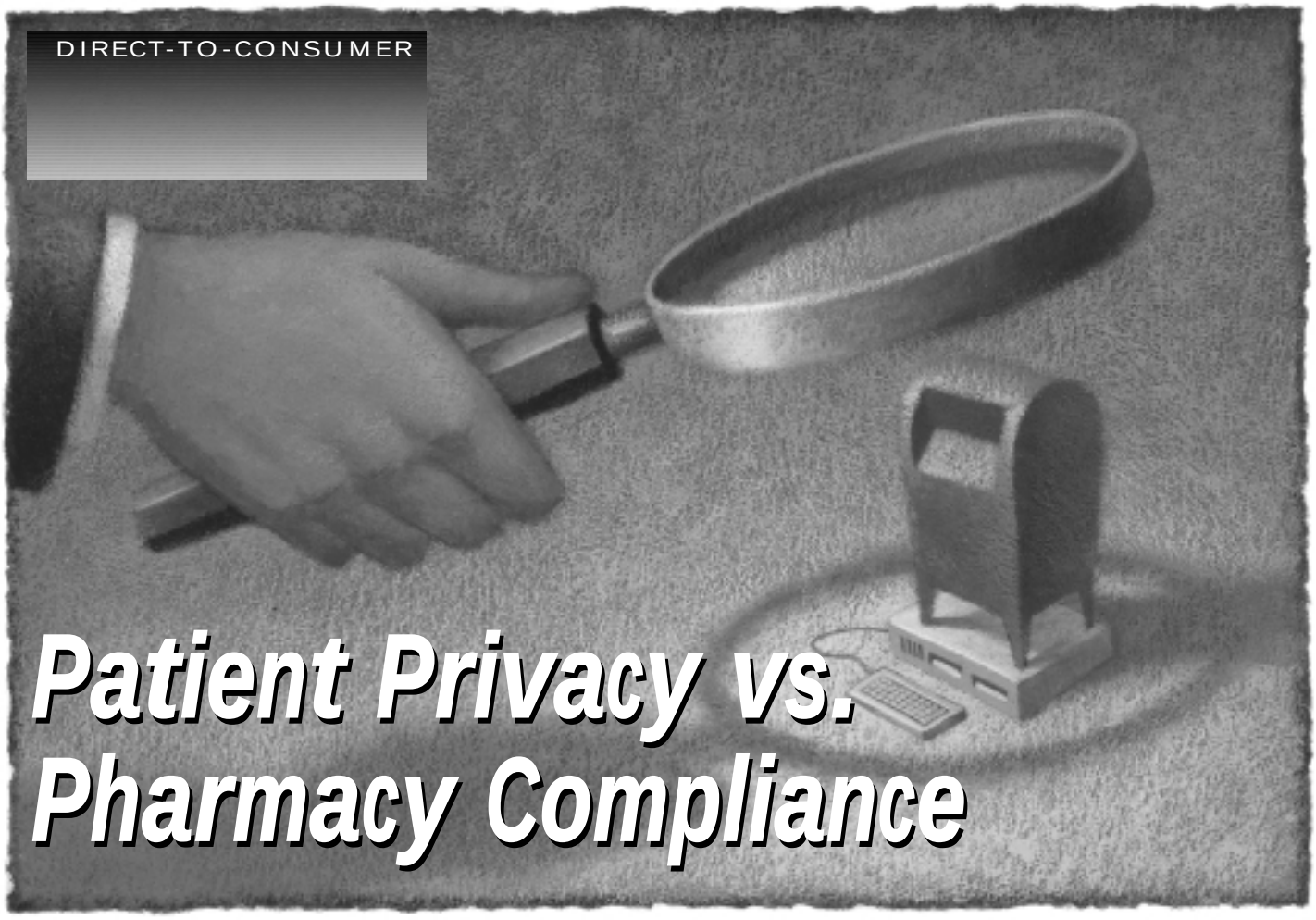


Patient Privacy vs. Pharmacy Compliance

Health Care Values Collide

As health information systems become more and more sophisticated, so too grows consumer concern over confidentiality. Adequate protection of data requires prior planning and purposeful implementation.

by Glenna Crooks, Ph.D.

Dr. Glenna Crooks, a former Reagan administration health policy advisor, is president of Strategic Health Policy International, which has offices in Ft. Washington, PA, and Washington, D.C.

Patient compliance and education programs sometimes receive rave reviews from patients. In late 1998, the National Wholesale Druggists' Association (NWDA) released survey results indicating that a majority of consumer focus group respondents aged 50 and older appreciate the educational literature they receive from pharmacies. Retirees, in particular, recognize that they are trading personal information for the compliance materials and feel that the exchange benefits them.

The NWDA study describes compliance programs as well-accepted by consumers. "The most important finding that can be derived from this survey is that respondents are highly receptive to unsolicited medication information/education that teaches them about innovative therapies for their condition," the report states. It also notes that one consumer reports that the material "makes it seem like someone cares about me."

Other studies have shown such programs are effective. In the Fleetwood Project, noted University of Arizona pharmacoeconomist J. Lyle Bootman, PhD, demonstrates that drug-related morbidity and mortality costs Americans nearly $76 billion per year—roughly the same amount they spend on drugs. Some estimates say that the cost may even be closer to $100 billion per year. Bootman estimates that pharmaceutical care programs could cut morbidity and mortality costs to about $30 billion a year. However, the implementation of programs that address these issues is endangered because the necessary consumer compliance information, currently stored in pharmacy computers, is at the forefront of debates on patient privacy.

This article describes how the pharmaceutical industry was blindsided by increasingly heated public policy conflict and offers ideas to help companies protect sensitive data. The conflict developed beneath

BIG BROTHER

A number of recent actions have taken place related to privacy concerns:

- In a move that privacy advocates regard as "scary," Iceland's Parliament voted in December 1998 to draw blood from each of its 270,000 residents for detailed genetic research and sell that information to Roche Holding AG for $200 million. It also voted to make available the contents of hundreds of years of its citizens' uniquely rich medical and genealogical records as part of the deal. Opponents have expressed concerns that this plan will spread to the rest of the European Union, despite EU's recent Privacy Directive.
- The medical and mental health records of a congresswoman from New York were faxed to a local newspaper during her campaign.
- The Harvard Community Health Plan kept extensive notes of psychotherapy sessions on a central computer accessible to all clinical employees.
- Sales representatives of a managed care company in Maryland were able to illegally purchase the electronic records of Medicaid recipients from eight Medicaid clerks.
- A purchaser of a secondhand computer discovered that the hard drive contained a grocery store's pharmacy records including patient names, addresses, Social Security numbers, and prescription medicines.
- During the Reagan administration, members of the U.S. Congress threatened to embarrass AIDS patients and leverage anti-gay sentiments at that time by reading medical records of AIDS patients treated at the National Institutes of Health Clinical Center on the floor of the Congress.

the surface and is now gaining mention more frequently in the mass media. Research, marketing, public affairs, and other influential executives throughout the industry need to become educated so they can participate more effectively in the public discussions and controversies that will escalate during next year's elections and into the 21st century.

THE INITIAL VOLLEY

Much of the recent public debate was incited by a 15 February 1998 front-page article in the *Washington Post* that erroneously suggested that CVS and Giant pharmacies had sold customer lists to Glaxo Wellcome. The story reported that pharmaceutical companies were using such lists to persuade pharmacy customers to buy the company's drugs. It also reported that Elensys, a Massachusetts company that delivers compliance and educational literature on behalf of these pharmacies, had participated in a scheme that violated the privacy rights of the patients whose records were in the pharmacy computers. (See *DTC Times*, May 1998.)

The *Post* articles reported that Elensys operated marketing and switching programs for pharmaceutical companies and reinforced that accusation in a February 18 editorial. On February 19, the *Post* printed on page 18 a retraction explaining that Glaxo Wellcome did not receive patient information, but the damage had already been done.

The public responded to the inaccuracies in the stories. Patients flooded the pharmacy with complaints, leading CVS to terminate its program and Giant to halt one that it had planned. Newspapers and television stations around the United States picked up on the *Washington Post* report, touching off a larger wave of negative media publicity. The media slant on this issue was not only misinformed; it was anti-industry. Within days, a CVS customer filed a class action suit in Massachusetts Superior Court naming CVS, Elensys, and Glaxo Wellcome as defendants. That lawsuit has since expanded to include Warner-Lambert, Merck & Co., and Hoffmann–La Roche.

Ultimately, the public's perception of the privacy issue is likely to drive state and federal legislation. A negative perception of the pharmaceutical industry's use of data could hamper the industry's ability to access the kind of patient information that informs research, drug development, post-marketing surveys, and educational efforts. Most importantly, laws that stunt the effectiveness of the health care industry disadvantage the patient and fuel the rising cost of health care to society.

The *Post* story was one of several events that crystallized the issue of patient privacy for the pharmaceutical industry. How this issue plays out in the mass media, the legislatures, policy arenas, and in the courts will determine whether patient data remain available for research, patient care, and cost-effectiveness studies and, if so, the form of this data. Virtually all health care analysts today believe that patient data are required to satisfy payer and public demands for the highest quality care at the lowest possible cost. Some analysts believe a generation must pass before we have accumulated enough accurate and statistically defensible demographic information for its use to be truly valuable in outcomes measurement.

The media slant on this issue was not only misinformed; it was anti-industry. The public responded to the inaccuracies in the stories.

TAKE TWO

The CVS/Elensys/Glaxo story was not just a single blip on the radar screen, appearing and then disappearing without notice. It was one of several seminal events that recently have highlighted the importance of the privacy issue.

In the last legislative session alone, at least five major bills in the 105th Congress and more than 250 initiatives in states legislatures have addressed patient privacy protection. In October 1998, the European Commission implemented its Privacy Directive, a measure that prohibits member states from transferring any data, including health care data, to any other country unless the recipient country has adequate privacy controls. The U.S.

Department of Commerce has suggested that American industries can self-police through voluntary internal guidelines, but some privacy activists regard that response as inadequate.

The Health Insurance Portability and Accountability Act of 1996 (HIPPA), also known as the Kennedy-Kassebaum bill, requires that Congress pass privacy legislation by August 1999. If it fails to do so, the secretary of the Department of Health and Human Services must impose regulations regarding data privacy by February 2000. (See Washington Report, January 1999.) Knowledgeable observers believe both deadlines will slip because stakeholders have yet to deal with the tough issues involved.

Editorials warned of "womb to tomb" privacy invasions enabled by unique health care identifying numbers.

Finally, a series of hearings on health identification numbers for American citizens scheduled for last summer ended abruptly after public outcry. Improving health care failed to stand up well to the fears of "Big Brother" data-gathering conspiracies espoused by consumer advocates. Editorials from coast to coast warned of "womb to tomb" privacy invasions enabled by unique health care identifying numbers for every American.

Consumer advocates, however, are not just whistling in the dark. Privacy concerns are real, as indicated by a number of recent actions. (See "Big Brother.")

UNINTENDED CONSEQUENCES

These and similar events are creating the political will to deal with the tough issues in protecting privacy. As the issues come into clearer focus, the pharmaceutical industry will likely experience disrupted business practices, increased costs, and a less positive public image. Federal and state efforts to legislate this area may create a patchwork of laws that may be particularly troublesome for companies operating across state and national lines—virtually everyone in health care today.

Although valuable research and clinical practice efforts are not the target of privacy protections, their implementation could be impeded by unintended effects of poorly conceived laws and regulations. Legislation buttressed by incomplete or poor policy debates will likely impair the ability of the health care system to function optimally for the patient. In their strictest interpretation, some proposed legislative initiatives could make it illegal to even send a drug recall letter to a patient. Several pieces of legislation that contain many of the same provisions as initiatives proposed last year have been introduced in the current Congressional session.

Restrictions on the collection and use of patient data could adversely effect the ability of pharmaceutical companies to access valuable information about post-marketing product use. Historically, investigators draw research subjects from small, self-selected populations. Access to large banks of patient information broadens this knowledge base and advances research and development. The ability to gather accurate and complete patient data from first encounter through final health outcome advances the study of therapies that work most quickly and at the least cost. The patient is the ultimate beneficiary of that information.

DEFINING THE TERMS

In talking about patient medical records, the terms *privacy*, *confidentiality*, and *security* often are used interchangeably though they have different definitions. Privacy is the right of the patient to have personal information kept secret and out of the reach of others, including health providers. Confidentiality is the protection of voluntarily disclosed private information from dispersal to persons not directly involved in providing care, both within and outside health care settings. Security includes the policy, procedures, and technologies intended to ensure that persons with access to patient information maintain privacy and confidentiality.

Suppose a patient seeking a diagnosis for an illness permits a health care provider to draw and test blood for a suspected condition—for example, hypercholeterolemia. The patient's right to privacy dictates that the health care provider test only for cholesterol level and not for other conditions—HIV infection, drug use, genetic conditions—on its own or at the request of another party such as a law enforcement agency, an employer, or a health insurer. Confidentiality protections dictate that the results of the cholesterol test not be disclosed outside the patient–caregiver relationship without the patient's permission. Policy and procedures related to the acqui-

In their strictest interpretation, some proposed legislative initiatives could make it illegal to even send a drug recall letter to a patient.

sition of permission for data release, the storage and transmission of medical records, and the granting of provider access to test information form the basis for the security of which the patient is assured.

The distinctions among privacy, confidentiality, and security are increasingly important to both the average citizen and mainstream policy debates. Although those issues were once the purview of academics and scholars of constitutional law, average citizens now have a stake in the discussions. Resolution of debate in the public arena will affect the quality and cost of health care into the next millennium.

Some areas of care may suffer in the wake of fears of greater exposure. Mental health records, HIV/AIDS status, genetic predisposition to health conditions, and medical conditions or disabilities that might impair employment or the procurement of health and life insurance will be among the most sensitive of patient information. Other classes of information will elicit a similar reaction. Even patients with more common and less stigmatized diseases will fear that the diagnosis of a disease will result in the loss of employment or insurance.

The 1993 Harris/Equifax study estimated that 11 percent of health care is "off the books" for just that reason. Proposals by the Clinton administration are based on the assumption that anyone receiving health insurance reimbursement should submit to the collection of information for research and quality improvement purposes. Other administration proposals would require that even cash transactions between patients and providers be recorded for tracking and research as well.

Mental health records, HIV/AIDS status, and genetic predisposition to health conditions will be among the most sensitive of patient information.

DEVIL IN THE DETAILS

Many can agree with a set of principles, developed by Department of Health and Human Services Secretary (HHS) Donna Shalala, that will serve as the foundation for the impending debates on privacy. Those principles dictate that health data collectors protect data and use it only for health purposes, that patients should have control over their data—including being able to correct it—that patients should be willing to share de-identified confidential information for improved understanding and care management, and that providers who disclose data without permission should face punishment. The real question is how long this agreement will last when the debate turns to practical and programmatic realities and the writing of regulations. Few health care businesses are prepared to address the devil in the details of privacy and confidentiality.

Potential solutions must take into account financial and credibility costs. Some observers predict that the cost to implement the confidentiality and security provisions recommended by Shalala will at least equal the cost of Y2K compliance and that at even this cost, the completeness and soundness of the data sets will be questionable. In just one recent example, Mayo Clinic paid nearly $7 million to collect signed informed consent forms from patients residing in a suburban county to satisfy a Minnesota state confidentiality law. Only 94 percent of patients agreed to the use of personal information, eroding the confidence some researchers will have in the completeness of the data.

Practically speaking, the debate in policy and programmatic terms will center on six major issues.

Data collection & use. Regulators must determine the types of information data collectors may gather, whether collectors may use identifiers, and how collecting parties may use it. Other questions to be resolved include: Must patients consent to the use of their medical records in health outcomes research? Should law enforcement be allowed access to records? Will pharmacies be prevented from using information contained in their data bases to monitor compliance and educate their customers?

Data management. How will collectors of data manage records to preserve privacy, confidentiality, and security? Does a patient have a right to privacy on all medical matters, including communicable diseases? Must all patient releases be in writing? Once a patient discloses private information, how long must collectors maintain confidentiality? Should those using confidential information be subject to criminal background checks? Should data disclosure be required as a condition for receiving health insurance coverage?

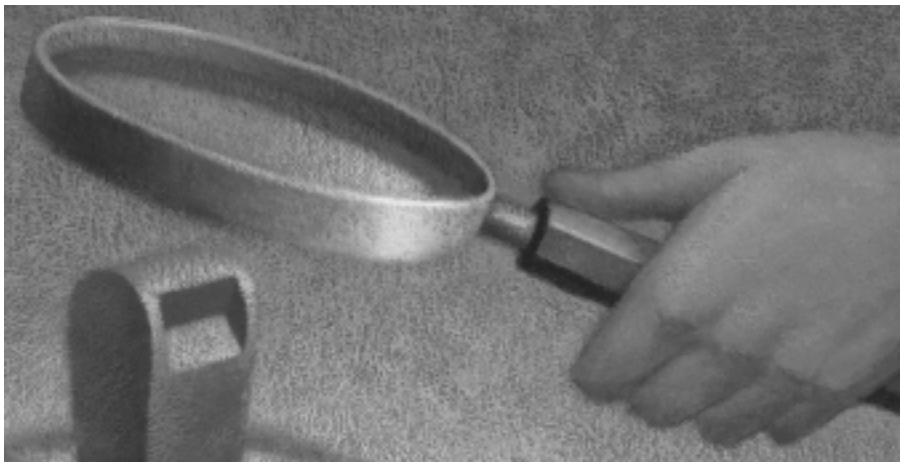
Patient rights. What rights will patients have to view and correct medical records? Who will prevail if a patient and a physician disagree on information in the record? How will patients be allowed access to records? If data collectors share uncorrected records and the patient later learns of inaccuracies, must collectors send all prior recipients the corrected information?

Limits of authorization. How detailed must the patient's consent be? Should consent be required for each use of the patient's data? Should patients be reimbursed for the use of the data? Should patients be required to opt in or opt out of pharmacy monitoring and compliance programs?

Few health care businesses are ready to address the devil in the details of privacy and confidentiality.

Penalties. How will regulators punish intentional and unintentional violators of data protection policies? Are individuals as well as corporations responsible for violations? Should regulators license data managers and repositories? Will pharmacists or the pharmacy be held responsible for the confidentiality its patient records?

Federal preemption. Will federal laws preempt state laws? Should federal laws create a "floor" over which state legislators may impose stricter laws? How



will regulators resolve conflicts between state insurance and federal privacy laws?

SUGGESTED STEPS

The debate surrounding medical privacy and confidentiality may well be one of the most complex and contentious policy discussions since the Clinton proposals for health care reform. It also may involve nearly as many people and enterprises. As a moving target on the policy agenda horizon with intense state legislative interest and federally mandated deadlines, this discussion merits watchful attention. It likely will create additional opportunities for attacks on health care providers, particularly those in the pharmaceutical industry.

Congress appears poised to miss its HIPPA deadlines, and medical privacy may well become an election issue because of the civil rights, constitutional protections, and states' rights issues it engenders. The nature of the risks requires providers' careful consideration. This is particularly true for pharmaceutical care providers and others developing new lines of information-based businesses, for which legislative and case law have yet to establish clear policy guidelines.

Pharmaceutical companies can take several steps to protect their financial assets and image as the debate wages. Company executives should discuss the following questions with their policy and business operations managers:

■ Has the chief information officer (CIO) established security provisions for the collection, maintenance, and transfer of health data within the organization? That should include training for all key personnel and monitoring adherence to the company's policies. New security rules proposed by the HHS secretary will require that companies have a responsible CIO, so companies that currently lack a CIO should create and fill this position.

■ What is the company data security policy? Does it include provisions for physical systems security, such as trusted personnel who have keys to computer areas? Is hardware under lock and key? Does policy restrict access to sensitive data on a role-based or need-to-know basis? Is information that crosses the Internet encrypted? Are all personnel trained in security awareness including password protection, and has their access been restricted to only that information necessary to do their jobs? Are audit trails established?

> At this juncture, companies will benefit from assessment of potential areas of vulnerability.

■ What are the consequences for policy violations? What are the consequences for security violations? Are they sufficiently severe that if the violation were to become public that consumers would agree it was adequate?

■ How are company operations affected in research, marketing, sales, customer service, and distribution? Does the application of various policy proposals concerning privacy and confidentiality place the company at any competitive advantage or disadvantage?

■ How do privacy, confidentiality, and security proposals affect new business initiatives? Is the company developing new products and services dependent on patient information? If so, companies should review those projects in light of privacy policy issues. The company should not make substantial investments without considering the risks to the business from policy shifts.

■ How active are industry trade associations? Does the company's key trade association keep its members informed of policy developments at the national and state levels? Are company interests in patient information–based products and services so substantial that the company should become directly involved in national or state legislative debates?

LONG VIEW

The privacy and confidentiality of patient records is an issue that may take 5–10 years to resolve. But many of the major stakeholders already are positioning themselves strategically for the discussions that will ensue. At this juncture, companies will benefit from assessment of potential areas of vulnerability. Additionally, companies must identify their information needs both for internal assessment and for external performance purposes.

As pharmaceutical companies assess their uses of patient data across the spectrum, from R&D to postmarketing outcomes studies, they should determine which business functions could become cumbersome or impossible as patient information protection regulations evolve. By identifying and quantifying vulnerable areas, companies can articulate their patient data needs to legislators and bureaucrats with greater clarity and authority. Laws that restrict the abuses rather than the uses of patient data will then be more likely to result. The ultimate beneficiary of good laws will be patients, whose medical information is protected from harmful uses while remaining available to agents undertaking legitimate efforts to develop more functional and cost-effective products. ❙

STRATEGIC
HEALTH POLICY
INTERNATIONAL, INC.

Glenna M. Crooks, PhD.

1075 Fort Washington Avenue,Fort Washington, PA 19034
(215) 646-8182 Tel (215) 646-7368 Fax GMCPP@aol.com