Health Information Policy: On Preparing For The Next War

Emerging information technology could escalate the ongoing war between cost and quality considerations in medicine.

by Donald W. Moran

PROLOGUE: One of the newest commodities in the health care marketplace is health information; close on its heels is the technology that is emerging to manage, move, and analyze that information. These tasks, in our complex, fragmented "nonsystem" of health care, are far from simple. As our nation moves headlong toward the twenty-first century, and as the development of technology products continues at breakneck speed, several issues arise that merit a pause in the action to ponder them. Chief among them is the role of managed care plans as managers of consumers’ information as well as their care.

The issues Donald Moran discusses in this paper have been the subject of much discussion on Capitol Hill and in the states, as lawmakers attempt to convert to legislation the patient protection and privacy provisions in President Clinton’s Consumer Bill of Rights and Responsibilities. First among those provisions was disclosure of performance information by health plans and providers. In this paper Moran argues for a "conscious health information policy" to shape our nation’s progress, rather than leaving the issues on a battlefield among stakeholders, from which the consumer might well emerge the loser.

Moran founded the Moran Company in 1998, which, among other activities, helps its clients to form new business ventures in the health care field. He previously worked for the Lewin Group, a consulting firm in Fairfax, Virginia, and served for several years as executive associate director for budget and legislation in the Office of Management and Budget during the Reagan administration.
ABSTRACT: As policymakers demand more and better information about health care, the private health information technology industry is investing heavily to produce the "paperless clinical enterprise" of the future: the infrastructure that will be required to satisfy those demands. Developments on a number of policy fronts, however—from medical privacy legislation to clinical software regulation to "telehealth"—suggest the need for a conscious health information policy that will inform the debate in each niche area with a larger sense of whether public policy will promote or retard private innovation in this area. Given the stakes involved, and the immediacy of the issues, leadership in this direction is badly needed.

To the extent that public policy rhetoric can be judged a leading indicator of underlying reality, the nation seems poised for a dramatic increase in the role that advanced information and communications technologies will play in our health care system. In every area of health policy, the debate is taking cognizance of the critical importance of information and the necessity of building the health care system's information technology infrastructure to supply it. Scarcely a day goes by in Washington's health policy community without some recitation of the demand for evidence-based assessments of clinical practice, report cards, guidelines, patient risk education programming, and a whole host of other applications that will require a dramatic upgrade in our ability to gather and assess clinical data. The vocabulary of the average health policymaker has expanded to include such previously abstruse topics as medical informatics, teleradiology, and Internet-based management of computerized medical records information. Conventional wisdom now holds that the health care system will be transformed over the next few decades into a "paperless clinical enterprise" that will permit clinicians to synthesize and apply the sum of human medical knowledge at the patient's bedside through the medium of advanced information technology.

The private-sector role in systems development. The promise of these technologies has not been lost on the private sector. Information technology spending in health care (at around 2 percent of industry revenues) has lagged well behind spending in other information-intensive industries such as banking and insurance (which spend 7-10 percent of revenues annually on information technology). Noting this, the Wall Street investment community senses a business opportunity poised to explode. Between 1992 and 1996 the number of publicly traded health information technology companies increased more than fivefold. The thirty-five companies in this field trading in the public-equity markets in the spring of 1998 commanded market capitalization in excess of $25 billion.

This growth in private-sector investment in health information...
technology reflects the fact that the great majority of product innovation and development activity that will build and install the emerging health information infrastructure will arise from the motive for profit. Although much of the intellectual and development work underlying health care informatics to date has been done within the academic medical and research communities, translating those ideas into viable systems will be largely a commercial effort. The component parts of the "paperless clinical enterprise"—and the infrastructure that will link those parts together into a coherent, functioning system—will be a blend of health care-specific applications and generic technologies put together by software application vendors and systems integrators.

The products now being developed by the private health information technology industry run across the full gamut of tools that will wire the clinical enterprise. Dozens (if not hundreds) of companies, large and small, are engaged in the development of various aspects of the technical solutions that will be required to build the technical components of the hardware and software infrastructure. Some companies concentrate on discrete aspects of the required technology, such as providing ways for clinicians to originate data in digital form. Others concentrate on paperless solutions for discrete clinical components, such as the "paperless radiology department." Still others are developing specialized data warehouse applications that will permit digital data from these various sources to be tied together into a system in which clinical information originating anywhere in a clinical enterprise is almost instantly accessible to caregivers elsewhere in the organization. When these efforts are viewed together with the efforts of companies engaged in "knowledge engineering" to mine the growing supply of digitized clinical data to support outcomes-based reengineering of clinical processes, it is clear that the technology base required to support policymakers' ultimate vision is moving off the drawing board and into production through the commercially motivated efforts of the private sector.

Is trouble brewing at the border? Given this apparent commonality of interest between the interests of policymakers and the motives of the private sector, it might appear that we are poised on the brink of a dramatic new era in health care, in which the power of emerging computing and telecommunications technologies synergistically combines with rapid advances in the biological sciences to produce a quantum leap in our ability both to treat disease and to promote rapid and continuous improvement in the efficiency of clinical processes.

Before concluding that we are on the brink of health information enlightenment, however, we must acknowledge a number of develop-
ments taking place at the boundary between the public and private sectors with respect to health information technology—developments whose net effect is to sound a cautionary note regarding our ability to achieve the full promise of these technologies.

In the short run, these developments amount to border skirmishes between the private-sector actors promoting rapid development of new health information technologies and the public-sector entities whose policy development agenda may create roadblocks, intentional or otherwise, to rapid technological development. Policy developments over the past few years in three key areas—medical privacy legislation, software regulatory policy, and telemedicine—illustrate that the road to the paperless, information-rich health care system of the future will be less than smooth.

To date, the debate in each of these areas has proceeded piecemeal, tracked by a narrow group of policy aficionados in each area of inquiry. The way that these debates are proceeding, however, suggests that there exists a larger policy debate, about what this all adds up to, in which we should engage before we march too far down any of these roads in any particular direction. As I suggest below, this debate awaits leadership. The purpose of this paper is to provide readers in the policy community with an outline of the issues likely to arise if, and as, this debate is fully joined.

Implications Of Medical Privacy Legislation

The medical privacy debate has arisen over the past few years as a natural consequence of the growing openness of medical information systems, as they transform from stacks of paper lying in locked filing cabinets into digital data accessible through an ever-widening array of portals.

The basic premise of privacy advocates in this debate is probably noncontroversial: that access to information about individually identified patients should be restricted to only those with an official “need to know” the information for purposes of managing a patient’s care. In considering potentially promising applications of health information technology, it is important to observe that many—and perhaps even most—are not inconsistent with even strong forms of individual medical privacy protection. Many of the things that health care informatics developers want to do with automated clinical data, such as population-based studies of the efficacy of alternative care processes, can be done with “blind” or “scrambled” patient identifiers that can permit the data to be used without compromising the privacy of individual patients.

Controversy nevertheless arises in this area, because a variety of things that need to be done with patient-specific information can-
"In the emerging medical privacy debate, the real issue is not security, per se, but rather data control."

not, for various reasons, be done with blind data. The demands of many care-related activities, ranging from payment system administration to fraud-and-abuse detection, require the ability to move patient-specific data outside the care setting. From a technical standpoint, the ability to match patient data from disparate sources in order to produce composite records requires the transport of patient-specific data across boundaries, even if the ultimate objective is to produce research data sets that will be used “blind.”

To the extent that movement of patient-specific data outside the care setting raises concerns about the security of the data, technical means are available to address these concerns. A nation that has the capability to safeguard sensitive national security information despite the concentrated attention of technologically sophisticated hostile powers probably has what it takes to keep genetic-testing results out of the hands of insurance underwriters. In the emerging medical privacy debate, the real issue is not security, per se, but rather data control.

Advocates of strong forms of medical privacy advance the view that patients should have the ability to deny access to their records to virtually any third party, and/or to require segmentation of their data to prevent disclosure of sensitive matters (for example, data regarding their mental health). Advocates of this view, moreover, typically seek to prohibit various actors in and around the health care system from inducing disclosure by conditioning participation in various activities on the patient’s affirmative decision to waive these rights.3

Although proponents of medical privacy see important matters of principle in these issues, developers of health care informatics applications see the potential for chaos. If every automated query to a database containing patient-specific information were to trigger an administrative action to authorize the disclosure, the administrative burden probably would be insurmountable. Even if administrative issues could be set aside on the grounds that the worst imaginable solutions could be avoided, there is still the question of whether “subject-edited” medical records data could be relied on as a source of authoritative information about anything meaningful.

Another manifestation of tension results from the recent concern over the use of “push” techniques in health care, whereby health benefits managers, using patient-specific health information, iden-
tify candidates for potential interventions and reach out to patients to invite their participation in those activities. Consider the controversy generated early in 1998 when it was discovered that several chain pharmacies had disclosed patient-specific data to companies interested in prodding patients to refill their prescriptions, with the consequence of stimulating increased drug sales. Although the backlash from that event suggests a potential political consensus around prohibiting such “push” tactics when they are motivated solely for commercial purposes, it is possible to visualize applying those techniques to a wide variety of applications whose intent is less obviously commercial and more directly aimed at improving the patient’s health. Across the health information industry, several dozen companies are investing substantial capital in the development of “push” applications designed to support targeted health risk identification and management strategies. Should public policy encourage such efforts or prohibit them? In the policy debate on health information issues up to this point, there is no apparent sign of a consensus answer to these sorts of questions.

Implications Of Software Regulation

While the privacy-versus-technology debate rages on, the U.S. Food and Drug Administration (FDA) and the health information technology industry are locked in a separate room down the hall quietly arguing about the appropriateness of regulating clinical decision-support software as a medical device under the Food, Drug, and Cosmetic Act (FDCA). These discussions are not, in my experience, closely followed by the health policy community, yet their subject matter has implications for the role of information technology that are exceedingly important to the question of how far we will go to realize the promise of these technologies.

Stripped to its essence, the issue is this: The FDA has long regulated the development and implementation of computer software whenever that software was embedded in a technology that was clearly a medical device. There is essentially no debate over whether the FDA has the power to do this, or about the applicability of the regulatory mechanism established under the FDCA to such software. The issue is whether the FDA’s authority, under the FDCA, also extends to software used in a clinical setting when that software is not integrally linked to a device that is itself subject to regulation. This issue is important in light of the fact that the health information technology industry is investing many millions of dollars in developing clinical decision-support software applications. These applications, intended to run in freestanding “physician workstations” in offices or at the patient’s bedside, are designed to support patient care and to reduce the burden of medical record keeping. Consider a situation in which doctors rely on these computer systems to coordinate patient care. To a large extent, the FDCA is a regulation of “black box” devices.

Given the FDA’s concerns about the policy implications of applying the FDCA to clinical software, would it make sense for an executive branch agency such as the NIH to create, with the two NICHD-funded software engineering centers on the West Coast, a “software engineering” effort required to make software development more practical and to safeguard the patient’s health?
support the automated retrieval and analysis of relevant information and to automate those aspects of clinical decision making that are reducible to prospectively determined rules. The issue under consideration is whether, at some point, the amount of "clinical thinking" done via the workstation has become sufficiently sophisticated to constitute the practice of medicine. It is easy to visualize that in many clinical settings in the near future, clinicians might come to rely on "what the box says" to make critical decisions about patient care. To the extent that they do, the FDA sees a clear mandate to regulate.

The FDA's view of whether such software is itself a "medical device," and hence subject to active regulation under the FDCA, turns on three critical issues. First, to what extent does the software permit clinicians to examine the underlying logic, to independently evaluate how the software arrived at particular findings and conclusions? Second, how proximate to the actual point and time of critical care decisions is the software application likely to be used? Third, how material are the consequences of error? The essence of the FDA position is that the closer an application comes to driving "black-box" conclusions in the real-time clinical setting, the closer the application comes to being a medical device.

Given the current state of policy regarding patient safety, the FDA thought process probably would resonate with many or most policymakers and would survive scrutiny as a reasonable framework for analysis. This framework, however, is not a clear and unambiguous policy in and of itself. Although it tells us that a "real-time black-box" application program clearly would be regulated, and that a "logically transparent office-based reference tool" probably would not be, it does not draw a bright line anywhere between these two extremes. As a result, the FDA's current view places the burden on the industry to err on the side of compliance with the 510(k) requirements in most cases. (Section 510(k) of the FDCA presents the regulatory mechanism for device regulation.) The challenge here is that the FDA has not had a very easy time figuring out what software manufacturers have to do to comply with the 510(k) requirements.

The 510(k) regulatory apparatus is based on an industrial engineering model that is appropriate for hardware manufacture but represents at best a strained analogy to the realities of software development. Anyone who has ever interacted with the cadre of besneaked Gen-Xers that inhabit the typical software development shop might wonder at the relevance of "good manufacturing practices" in such a setting. Although the rationale for regulation is to guarantee the public that a suitable degree of rigor is being applied to