The Practice of Informatics
JAMIA

Review ■

Serious Technology Assessment for Health Care Information Technology

Reid Cushman, PhD

Abstract United States health care is engaged in an ambitious project to make its clinical and administrative records "100% electronic." Substantial benefits are expected in both clinical care delivery and medical research (especially for public health surveillance and outcomes/effectiveness studies). Substantial costs also potentially accrue, beyond the large outlays for an expanded computer and telecommunications infrastructure. Privacy and confidentiality are obviously at risk if such systems cannot be made secure. Limited empirical evidence currently available suggests health information systems security may not be very good, at least in the "average" institutional setting. Privacy-focused critics of electronic record-keeping are sometimes accused of taking Luddite stands, insufficiently attentive to IT's benefits. It may also be fair to worry about a certain Panglossian tendency in "industry" commentary, insufficiently attentive to potential problems. Better federal and state laws structuring health data use will help; the industry must also attend more candidly to the technical uncertainties.

■ **J Am Med Inform Assoc.** 1997;4:259–265.

The United States has had a hard time translating notions of health care equity into public policy for system-wide reform. On the efficiency side of the problem, however, there is now frenetic, predominantly private activity aimed at promoting "correct" behavior. Under the banner of "managed care" come structures of co-payments and deductibles for consumers; a fine-tuning amongst fee-for-service, capitation, salary, and incentive regimes for producers; and all manner of market "intermediary" institutions. Worldwide, there is a fervid quest for better information about the costs and benefits associated with the available range of drugs, devices, and procedures, so that the "correct" rates of application can be known. Limited attention to such technology assessment—particularly of the "is this worth what it costs" variety—was until rather recently a common, unacknowledged feature of health care. High rates of expenditure growth and the embarrassing discoveries of large practice variations forced the industry to admit that there was "insufficient evidence" about most interventions' "diagnostic, therapeutic, and ultimate health effects."[1]

New information technology (IT) applications are expected to play a key role in reducing the knowledge

Affiliations of the author: Robert Wood Johnson Foundation Health Policy Scholar, Institution for Social and Policy Studies, Yale University, New Haven, CT; Senior Research Associate of the Health Policy Center, University of Virginia, Charlottesville, VA.

Grant support by Robert Wood Johnson Foundation, full salary support, academic years 1995–96 and 1996–97.

Correspondence and reprints: Reid Cushman, Institution for Social and Policy Studies, Yale University, 89 Trumbull Street, P.O. Box 208207, New Haven, CT 06520-8207.
E-mail: reid.cushman@yale.edu

Received for publication: 8/28/96; accepted for publication: 2/17/97.

deficit. As most readers here are well aware, large-scale aggregations of computer-based clinical and administrative records are presumed to be a growing source of data for outcomes research. Database and decision-support tools, interfacing with electronic patient records, may someday be a principal mechanism by which research results are fed back into clinical choices.[2] It is thus ironic that health care IT itself sometimes seems to be a last bastion of the old-style technology *non*assessment that it will be used to eradicate. Great claims are not uncommonly made for new "automated" systems, without much clear proof of the magnitude of benefits and with sometimes limited attention to the explicit and implicit costs. Even the Institute of Medicine's widely respected report entitled *The Computer-Based Patient Record: An Essential Technology for Health Care* gives rather short shrift to matters of cost: "likely to be substantial but . . . difficult to estimate," it quickly concludes.[3]

The explicit price will of course be substantial—tens of billions of dollars a year, just for the computer and telecommunications infrastructure. Yet the more important cost may be the implicit one if these systems are not made secure. Given the volatile personal information commonly embedded in health records, an atmosphere of distrust about the security of computer-resident data inevitably breeds fears of personal humiliation, loss of reputation, and risks to financial status. This is particularly so in the United States, where weak antidiscrimination and privacy protections coincide with the strong discriminatory incentives of private finance. The recent Kassebaum–Kennedy health insurance "portability" legislation may ensure greater coverage continuity, at least for those in employer groups, but its only partial limits on insurance pricing preserve many of the incentives to pick and choose those with better health.[4] Likewise, the antidiscrimination protection of bodies like the Equal Employment Opportunity Commission (EEOC) are at best only partial.[5]

Fuller protection also awaits passage of national "data protection" legislation to replace a crazy quilt of inadequate state and federal "privacy" law that largely fail to govern a growing traffic in health care information.[6] This congressional session's controversies over the Bennett–Leahy, McDermott, and "administrative simplification" proposals show the task will not be an easy one.[7] In the interim, patients' entirely rational confidentiality fears may cause them to increasingly withhold sensitive information from their health care providers. Such nondisclosure presents obvious personal risks, since it could materially affect the course of care. Equally, physicians may feel forced into keeping some types of data out of patient records (or keep duplicate, private records of sensitive information). Incomplete or inaccurate records have the potential to contaminate the knowledge base for outcomes research and surveillance. Sorting out privacy and confidentiality requirements—and putting in the security mechanisms to ensure they are met—is thus not just an engineering puzzle or an ethical "nicety." It is a matter that potentially conditions the abilities of the clinical and research apparatuses of health care to perform appropriately.

Weighing Alternatives Seriously

Performance predictions for unprecedentedly large, ambitious information system designs are not uncommonly wide of the mark. Consider the U.S. military's difficulties in implementing its own $2.8 billion worldwide electronic medical record (EMR) system.[8] In fact, IT benefits specifications can be elusive even when the design mark is hit. Productivity and investment return are notoriously difficult to measure for computer and telecommunications investments, particularly in service industries like health care. As a National Research Council study put it, "[p]ayoffs . . . are likely to be uncertain in both scale and timing . . . [e]xpected value is often not quantifiable or even estimable, let alone predictable."[9] These frustrating uncertainties have often led to limited or nonexistent IT cost–benefit analyses. The U.S. government's IT cost–benefit practice has been notably lackluster despite the requirements of law and regulation.[10]

In the case of EMR systems, improved clinical decision making logically flows from faster access to richer patient-specific data. Yet the fraction of patients for whom the improvement will be substantial, particularly enough to justify the large associated costs, is not yet known. The very sick, intensively cared for patient in a hospital environment represents a paradigmatic case. So does the "emergency" patient, acutely ill, far from home, and with a complex medical history. Could we serve such patients equally well with intrainstitutional EMRs, distributed data vehicles like smart cards, and a regimen of only very limited networking? On the research side, the ultimate usability and cost of outcomes research data, derived from large-scale records mining, is also unclear.[11] Public health-oriented surveillance may well be assisted substantially.[12] But hopes that such data amalgamations will be a cheap, high-quality substitute for controlled trials have to date not been realized.[13] Could we perhaps make do with less exhaustive, more focused population databases? To what extent could we rely on "anonymized" (unidentifiable) patient rec-

ords? Most critically, could we preserve a right for patients to "opt out" of some data uses without unacceptable compromises to data quality?

Given what is at stake, one might expect a cautionary, experimental approach to such questions. Instead, nationally and even globally networked databanks of cradle-to-grave records constitute the modal aspiration. ("Master patient indices" are planned to link these data repositories, at least until a "universal health identifier" can be put in place.) The prevailing belief is that the medical benefits of such systems outweigh security risks and that the health sector is too far behind in its "automation" to go slow now. That belief may well be correct, but it seems grounded on rather thin empirical evidence to date. Moreover, we know little about the actual state of health care information systems security today, about the nature and scope of both legal and illegal information traffic, or about the discriminatory behaviors that occur based on that information. In short, we have a limited "threat model" on which to ground systems design, even though we have seen the problem coming for a long time.[14]

For health care generally, technology assessment lagged behind sector growth, in part because of historical factors: Until late in this century, practitioners could offer few interventions, fewer still that did much good; nothing cost very much, at least as measured by today's standards; and reimbursement regimens provided little incentive for self-discipline. Yet practitioners now pay a steep price for their technology assessment failings. Managed care controls have been increasingly imposed from the "outside," by public and private payers, in sometimes very unpleasant ways. Health care IT applications have lagged behind sector growth as well, especially compared with industries like banking and finance, with isolated systems and limited functionality the norm.[15] Now that the sector is "catching up" it should resist the temptation to give short shrift to careful assessment of IT itself. Information technology's importance in "leveraging" other efficiencies, its significant monetary costs, and its implications for privacy and discrimination all argue for flinty-eyed technology assessment. Practitioners otherwise risk losing control over health care IT, as they have, to no small degree, been supplanted in their direction of health care technology generally.

Practitioners' Views: One Example

Yet a sometimes subtle Panglossian tendency characterizes many "insider" IT evaluations. Consider an article in the March/April 1996 edition of this journal, entitled "Privacy, Confidentiality, and Electronic Medical Records," by Randolph Barrows, Jr., MD and Paul Clayton, PhD.[16] The authors are affiliated with the Center for Medical Informatics at Columbia–Presbyterian Medical Center (New York), an institution renowned for its advanced implementations of health care information systems, and are themselves prominent in the field of health care IT. *JAMIA* itself is aimed, by its own description, at a readership oriented to "the practice of informatics." The attention of such an audience for privacy and confidentiality concerns is surely welcome. Unfortunately, the article raises more concerns than it settles.

Barrows and Clayton laudably emphasize the importance of trust and confidentiality in health care interactions and the critical need for preservation of both. They discuss the "significant economic, psychologic, and social harm that can come" when personal information is disclosed, and they briefly itemize the "incomplete and inconsistent" current legal protections for privacy in the United States. While "applicable security technologies exist," borrowed from the banking and military sectors, the authors note that "experience is lacking" about the transferability and effectiveness of these regimens for the health environment. They discuss the intolerance within many health care facilities of inconveniences associated with security practices, and they remark that even their own institution had difficulty making sound administrative policies to complement technical safeguards. Indeed, though Columbia–Presbyterian appears to be a model of good IT security, the authors note that many institutions could not meet the proposed 1995 information management standards of the Joint Commission on Accreditation of Health Care Organizations (JCAHO). Consequently, the JCAHO requirements were "downsized" with the "stated intention of a more gradual deployment."

While "awareness of risks and of possible technical solutions is increasing," the authors would appear to be describing a rather precarious environment, at least in the short run. The picture does not improve when one focuses on the details of some of the technical fixes. Barrows and Clayton deem "tight" prospective access restrictions—a "need to know," mandatory access control model—as largely incompatible with the dynamic health care environment.[17] Columbia–Presbyterian itself implements a limited access control matrix (classifying users as attending physicians, residents, medical students, hospital nurses, and so forth), with differing access privileges granted for each group. But the authors admit this offers fairly limited protection given the large number of users in each category: "[P]rohibition of access by most medical

users to most data on most patients is often not practical,'' they note. Instead the security model is based on ''need-to-show'' controls, with users disciplined by the potential requirement to show, after the fact, why their access to a particular patient's information was appropriate.

Good post hoc need-to-show security requires an appropriate audit trail facility, whereby significant system events are logged. Since such logging data are voluminous, they must be analyzed by computer-based techniques to have a reasonable chance of detecting problems; no human could parse them unassisted. And what of such tools, according to the authors?

> Statistical techniques lend themselves to anomaly detection but are inadequate to detect all types of intrusions and do not prevent users from gradually training their usage profiles, so that activity previously considered anomalous might be regarded as normal. Expert-systems and model-based techniques lend themselves to misuse detection, but specification of the ordering on facts, for the pattern matching of events, has been deleteriously inefficient. . . . Each system is out of necessity . . . somewhat ad hoc and custom designed. . . . *[N]o commercially available audit-analysis tool kit yet exists, and there is as yet no known application of software tools for audit analysis in the health care sector* [emphasis added].[18]

After the basic mechanics of identification and authentication (e.g., by user IDs and passwords), event logging and audit are the most important line of defense against access violations. But at least for now, in the average health care institution, it would seem to be a weak line.

The situation is little better with encryption. Barrows and Clayton note that ''for practical purposes, due to the embedding of sensitive data in text objects'' all health data should be encrypted. Encryption is also essential for ensuring that data is uncorrupted and that it came from the expected source (message accuracy and authentication, respectively). Again, however, there is a critical problem of technology availability. Cheap, effective cryptographic hardware and software have been slow to appear on the market, in part because of uncertainties about government export controls.[19] The authors note that

> [s]oftware tool kits for the secure transmission and archiving of files by medical applications are *beginning* to appear. In the near future, vendor products will supply encryption technology embedded within computer systems for health care. Until then, [EMR] developers are forced to create their own implementations of well-known and secure cryptographic algorithms and protocols. . . . *Cryptographic techniques applicable to the goals of privacy, integrity and access control have not yet been significantly deployed in the health care environment, and experience is needed before establishing that they could provide security solutions compatible with the diversity of health care needs* [emphasis added].[20]

As with audit trail mechanisms, a requirement for ad hoc implementation usually guarantees a low rate of utilization, since one-off designs are expensive (and requisite expertise can be unavailable at any price). Thus it is perhaps unsurprising that Ernst & Young's 1995 information security survey[21] found only about one-quarter of some 1300 reporting U.S. institutions regularly used encryption to protect data. The rate for the 134 health care respondents in the survey was even less impressive: only one in ten.

Given a precarious legal environment, a lagging and arguably recalcitrant institutional environment, and on-going availability and implementation deficits for critical security technologies, one might conclude there is cause for concern and a lot of caution. Barrows and Clayton conclude: ''[S]ubstantial advantages to the electronic record exist, and it seems prudent to move ahead with implementations of electronic records.'' We may worry that the real conjunction in this sentence is a ''therefore,'' not an ''and''—the vision of ''substantial advantages'' pressing the notion of ''prudence.'' Particularly given the incentives inherent in our private, risk-based system of health care finance, arguably no country presents as unsafe an environment for health data as does the United States today.

Relative Risks: Paper Versus Electrons

To be sure, security with paper systems has rarely been remarkably good, despite the long-standing requirements of certification bodies like the JCAHO.[22] Indeed, this is something proponents of EMRs almost always bring up in short order. Paper's typical problems are well known: inadequate access validation and ''logging'' procedures by file clerks to control and trace which records are sent where; defective physical security for central repositories, and for individual records as they move within and among institutions; and the omnipresence of the photocopier and fax machine to reproduce documents.[23] While this may be a partial defense of moving on to electronic systems, which at least will (someday) afford facilities like audit trails to trace use, it also raises an interesting counter question: Why have so few moved authoritatively to rectify the ''glaring'' security problems with paper records? The answer seems to be that such

protection has not been considered worthy of serious attention—or, more accurately, serious money. Information access has been the priority, secondary to the prime mission of care delivery.

Attitudes change a lot more slowly than does technology. We may presume that access considerations will continue to trump security concerns in many institutions as the sector moves to predominantly electronic environments. At least they seem likely to do so absent new legal or regulatory pressures. Barrows and Clayton remark that "[e]lectronic medical records are arguably more secure [than paper] if the proper policies and best available technologies are in place." Perhaps they mean the best soon-to-be-available technologies, but even granting the premise does not end the matter. First, unlike the place the authors inhabit, many institutions will likely be far behind the "best practices." In a networked world, security is often only as good as the weakest institutional link. While high-quality empirical data is lacking, there is ample reason to suspect that the average level of IT security in health care institutions is not very good and that, given deficits in expertise and monetary resources, the situation is likely to improve only slowly.[24]

Second, even an accurate "average" figure by itself tells only part of the story, given the well-known differences in risk structures. Paper records carry high probabilities of small (individual record) violations, but they carry low probabilities of large breaches given the physical difficulties of manipulation. Electronic environments inevitably carry significant nonzero probabilities of large information losses once a security breach has occurred. All the current federal data protection proposals would structure the patterns and privileges accorded to classes of health data users and attach penalties for misuse. But sharing of records among distributed institutions is likely to continue and intensify.[25] Ever-growing numbers of individuals will thus have access, as part of their official duties, to identifiable health records. Absent monitoring, such as with adequate audit trail regimens, such persons will have the ability to "mine" health record databanks with impunity.

Several recent incidents, such as the distribution of HIV/AIDS patient data by a public health agency employee in Florida, give a hint of the information Chernobyls that are increasingly likely.[26] Information leaks are not quite of the same class as radiation leaks, of course, though they share the characteristic of being very difficult to clean up after they have occurred. Yet one dramatic leak, whatever its actual consequences, has the possibility of substantially eroding the public's confidence—particularly a public with predispositions to superstition about new technology. (The recent controversy over Lexis-Nexis' P-Trak service suggests the potential volatility of public opinion.[27]) Trust is not an asset in particularly robust supply in today's rapidly changing health systems anyway, given the fallout from managed care. It will be a tragic irony indeed if information technology, intended to "save" health care by pointing a way toward greater efficiency, ends up substantially undermining the trust essential to system functioning.

Ludditism Versus Prudence

Only a true Luddite would advocate standing pat with paper until "absolute" security can be achieved. There is, of course, no such animal. The rational question is one of marginal adjustments—here, specifically, of our ambitions for the rate, scale, or scope of IT implementations. Security is expensive and has no natural constituency. When resources are tight, we know it is commonly a casualty. Hospitals are the logical epicenter of EMR implementations, with interhospital and intersystem networking following. (It is from hospital environments that we have the best evidence of IT productivity.[28]) In the United States, hospitals are under tremendous competitive pressure as the industry restructures under managed care—e.g., to a much greater level of outpatient services. Mergers, consolidations, and closures are expected to continue. Reimbursement levels from both private payers and government are continually ratcheting downward, narrowing profit margins for the surviving institutions. It would be hard to describe an environment less likely to have the discretionary resources for a robust investment in data security—even for current systems, much less ambitious new ones.

Beyond anecdotes, though, what hard evidence do we have about current threats? Not much. But the limited data provides little comfort. Consider that in the 1995 Ernst & Young survey,[29] 57% of the health care institutions responding reported an "information security-related loss" in the last 2 years, up from 54% in the preceding year's survey. (For all respondents, the figures were 54% and 53%, respectively.) Some 88% of the health care institutions considered that their security risks were worsening (85% for all respondents). Even granting that such responses may lump together both the negligible and the serious, those are high numbers. (Out of circumspection or simple inability, most respondents declined to estimate the dollar value of their losses.) The survey's data on security practices is just as unsettling. Health care respondents had on average very low rates of technical security measures (such as encryption). Health facilities also had low rates of complementary administrative practice (e.g., security awareness and training programs).

Despite this, health care institutions had a higher level of satisfaction with their own security effectiveness than any other industry included in the survey. With all the health sector's recent difficulties, it is at least good to know that self-esteem is not a problem too.

Other large-scale surveys of information security, each with its own methodological flaws, nonetheless point in a similar direction. Data protection practices in the typical late twentieth-century organization are not very good, even in putatively "secure" institutions like the U.S. Defense Department.[30] (The forthcoming study of health care security by the National Academy of Sciences, to be released in February 1997, is expected to reach a similar conclusion. Brief excerpts from that report will be put in this paragraph.[31]) The widespread deficits in security are hardly a secret; they are common fodder among information systems professionals. The oddity is that health care professionals who promote IT systems often persist in denying the problem exists, as though such news might be unduly frightening for the "patient."

Beyond the narrow confines of clinical care, the research and public health benefits of EMR systems are often generalized rather than individual; indeed, they are even intergenerational. But these systemic benefits tend to flow precisely from the practices that are potentially the riskiest with respect to individual privacy, such as broad networking, interchange, and aggregation of records for analysis. We are all experimental subjects now, given the uses to which our aggregated data may be put. We are all, also, part of an ongoing experiment in the efficacy and safety of the IT security practices for the systems in which our personal data will be stored. The protocol of this experiment will be fair to its subjects—that is, to all of us who are or will be patients—only if we proceed at an implementation pace consistent with our technical and organizational abilities.

A preliminary version of this paper was presented at the Isaac Newton Institute Conference on Personal Information Security, Engineering and Ethics (Cambridge University, UK, June 1996). The author is grateful for the comments provided by those who attended the conference and by other anonymous reviewers. Support for the author's research in information technology policy was provided by the Robert Wood Johnson Foundation. Ernst & Young, LLP, provided additional, unpublished data from its information security surveys.

References ■

1. Institute of Medicine, 1990. Modern Methods of Clinical Investigation. Washington, DC: National Academy Press, 1990.
2. For more details, see: Institute of Medicine. Health Data in the Information Age: Use, Disclosure and Privacy. Washington, DC: National Academy Press, 1994.
3. Institute of Medicine. Health Data in the Information Age: Use, Disclosure and Privacy. Washington, DC: National Academy Press, 1994.
4. "Kennedy–Kassebaum: What does it all mean?" Parts I and II. American Health Line, 11 and 23 September, 1996.
5. Mathews J. Disabilities act failing to achieve workplace goals. Washington Post, 16 April, 1995.
6. Kolata G. When patients' records are commodities for sale. New York Times, 15 November, 1995.
7. Data protection bills introduced in the 104th US Congress included: (1) Medical Records Confidentiality Act of 1995 (S.1360, introduced by Sens. Bennett and Leahy; (2) Medical Privacy in the Age of New Technologies Act (HR.3482, introduced by Rep. McDermott); (3) Genetic Privacy and Nondiscrimination Act of 1995 (S.1416 and HR.2690, introduced by Rep. Stearns and Sen. Hatfield); and the Genetic Confidentiality and Nondiscrimination Act of 1996 (S.1898). Provisions of the Health Coverage Availability and Affordability Act of 1996 (see subtitle F, "Administrative Simplification"), passed in August 1996, mandate study of health care privacy and security issues by the Department of Health and Human Services. The Bennett–Leahy bill, styled as a reasonable middle ground between the status quo and highly protective bills such as McDermott's, proved unacceptable to both "pro-industry" and "pro-privacy" factions.
8. General Accounting Office. Defense Achieves World-Wide Deployment of Composite Health Care System. Washington, DC: US Government Printing Office, 1996.
9. National Research Council. Information Technology in a Service Society, Washington, DC: National Academy Press, 1994.
10. Regan PM. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press, 1995.
11. Institute of Medicine, 1990.
12. Gostin LO et al. The public health information infrastructure: a national review of the law on health information privacy. JAMA. 196;275:1921–27.
13. Office of Technology Assessment. Identifying Health Technologies That Work: Searching for Evidence. Washington, DC: US Government Printing Office, 1994.
14. See the two examples cited by Barrows and Clayton: Hiller MD, Beyda V. Computers, medical records and the right to privacy. Journal of Health Politics, Policy and Law. 1981;6: 463–87; and American Medical Record Association, Position Paper on the Confidentiality of Medical Information, Medical Record News, December 1974.
15. National Research Council, 1994.
16. Barrows R, Clayton P. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc. 1996;3:139–48.
17. For a contrasting point of view, see Anderson RJ. Security in clinical information systems. Report for the British Medical Association, 1996.
18. Barrows R, Clayton P. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc. 1996;3:139–48.
19. Office of Technology Assessment. Issue Update on Information Security and Privacy in Network Environments. Washington, DC: US Government Printing Office, 1995.
20. Barrows R, Clayton P. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc. 1996;3:139–48.
21. Ernst & Young. Third Annual Information Security Survey: Trends, Concerns and Practices. New York, NY: Ernst & Young, 1995a; and Ernst & Young. Third Annual Information Security Survey: Trends, Concerns and Practices, A Fo-

cus on the Healthcare Industry. New York, NY: Ernst & Young, 1995b.
22. Joint Commission on the Accreditation of Hospitals. Acccreditation Manual for Hospitals. Chicago, IL: Joint Commission on the Accreditation of Hospitals, 1976.
23. Office of Technology Assessment. Protecting Privacy in Computerized Medical Information. Washington, DC: US Government Printing Office, 1993.
24. Ernst and Young, 1995a and 1995b; Riley J. Open secrets: changes in technology, health insurance making privacy a thing of the past. Newsday, 31 March 1996; van den Hoven, MJ, Cushman R. Conference report: conference on privacy, health care data, and information technology. Journal of Information Law and Technology. 3 September 1996.
25. Gellman R. Perspectives on Proposals for Federal Health Confidentiality Legislation in the United States. In: Visions of Privacy for the 21st Century: A Search for Solutions. Office of the Information and Privacy for the Province of British Columbia.
26. Tippett S. New danger in the age of AIDS: Florida health employee accused of sharing names in database.'' Washington Post, 14 October, 1996.
27. Lexis-Nexis P-Trak Service Gets Flak from Internet Newsgroup Misinformation. Online Newsletter, 1 October, 1996.
28. Pestotnik SL, Classen DC, Evans RS, Burke JP. Implementing antibiotic practice guidelines through computer-assisted decision support: clinical and financial outcomes. Ann Intern Med. 1996;124:884–90; Evans RS, Larsen RA, Burke JP, Gardner RM, Meier FA, Jacobsen JT, Hulse RK. Computer surveillance of hospital-acquired infections and antibiotic use. JAMA. 1996;256:1007–11; Tierney WM, Miller ME, Overhage JM, McDonald CJ. Physician inpatient order-writing on microcomputer workstations: effects on resource utilization. JAMA. 1993;269:379–83.
29. Ernst & Young, 1995a and 1995b.
30. Waning security. PC Week, 2 December, 1996; SATAN and security. New Scientist, January 1997; The price of security. PC Week, 20 January, 1997.
31. National Academy of Sciences, Data security assessment of health care organizations.