10
Ethics and Health Informatics: Users, Standards, and Outcomes

KENNETH W. GOODMAN AND RANDOLPH A. MILLER

After reading this chapter, you should know the answers to these questions:

- Why is ethics important to informatics?
- What are the leading ethical issues that arise in health care informatics?
- What are examples of appropriate and inappropriate uses and users for health-related software?
- Why does the establishment of standards touch on ethical issues?
- Why does system evaluation involve ethical issues?
- What challenges does informatics pose for patient and provider confidentiality?
- How can the tension between the obligation to protect confidentiality and that to share data be minimized?
- How might computational health care alter the traditional provider–patient relationship?
- What ethical issues arise at the intersection of informatics and managed care?
- What are the leading issues in the debate over governmental regulation of health care computing tools?

10.1 Ethical Issues in Health Informatics

More and more the tendency is towards the use of mechanical aids to diagnosis; nevertheless, the five senses of the doctor do still, and must always, play the preponderating part in the examination of the sick patient. Careful observation can never be replaced by the tests of the laboratory. The good physician now or in the future will never be a diagnostic robot. (The surgeon Sir William Arbuthnot Lane writing in the November 1936 issue of *New Health*)

Human values should govern research and practice in the health professions. Health care informatics, like other health professions, encompasses issues of appropriate and inappropriate behavior, of honorable and disreputable actions, and of right and wrong. Students and practitioners of the health sciences, including informatics, share an important obligation to explore the moral underpinnings and ethical challenges related to their research and practice.

Although ethical questions in medicine, nursing, human subjects research, psychology, social work, and affiliated fields continue to evolve, the key issues are generally well

known. Major questions in bioethics have been addressed in numerous professional, scholarly, and educational contexts. Ethical matters in health informatics are, in general, less familiar, even though certain of them have received attention for decades (Szolovits and Pauker, 1979; Miller et al., 1985; de Dombal, 1987). Indeed, informatics now constitutes a source of some of the most important and interesting ethical debates in all the health professions.

People often assume that the confidentiality of electronically stored patient information is the primary source of ethical attention in informatics. Although confidentiality and privacy are indeed of vital importance and significant concern, the field is rich with other ethical issues, including the appropriate selection and use of informatics tools in clinical settings; the determination of who should use such tools; the role of system evaluation; the obligations of system developers, maintainers, and vendors; and the use of computers to track clinical outcomes to guide future practice. In addition, informatics engenders many important legal and regulatory questions.

To consider ethical issues in health care informatics is to explore a significant intersection among several professions—health care delivery and administration, applied computing, and ethics—each of which is a vast field of inquiry. Fortunately, growing interest in bioethics and computer-related ethics has produced a starting point for such exploration. An initial ensemble of guiding principles, or ethical criteria, has emerged to orient decision making in health care informatics. These criteria are of practical utility to health informatics.

10.2 Health-Informatics Applications: Appropriate Use, Users, and Contexts

Application of computer-based technologies in the health professions can build on previous experience in adopting other devices, tools, and methods. Before they perform most health-related interventions (e.g., genetic testing, prescription of medication, surgical and other therapeutic procedures), clinicians generally evaluate appropriate evidence, standards, presuppositions, and values. Indeed, the very evolution of the health professions entails the evolution of evidence, of standards, of presuppositions, and of values.

To answer the clinical question, "What should be done in this case?" we must pay attention to a number of subsidiary questions, such as:

1. What is the problem?
2. What am I competent to do?
3. What will produce the most desirable results?
4. What will maintain or improve patient care?
5. How strong are my beliefs in the accuracy of my answers to questions 1 through 4?

Similar considerations determine the appropriate use of informatics tools.

10.2.1 The Standard View of Appropriate Use

Excitement often accompanies initial use of computer-based tools in clinical settings. Based on the uncertainties that surround any new technology, however, scientific evidence counsels caution and prudence. As in other clinical areas, evidence and reason determine the appropriate level of caution. For instance, there is considerable evidence that electronic laboratory information systems improve access to clinical data when compared with manual, paper-based test-result distribution methods. To the extent that such systems improve care at an acceptable cost in time and money, there is an obligation to use computers to store and retrieve clinical laboratory results. There is less evidence, however, that existing (circa 2006) **clinical expert systems** can improve patient care in typical practice settings at an acceptable cost in time and money.

Clinical expert systems (see Chapter 20) are intended to provide decision support for diagnosis and therapy in a more detailed and sophisticated manner than that provided by simple reminder systems (Duda and Shortliffe, 1983). Creation of expert systems and maintenance of related knowledge bases still involve leading-edge research and development. It is also important to recognize that humans are still superior to electronic systems in understanding patients and their problems, in efficient collection of pertinent data across the spectrum of clinical practice, in the interpretation and representation of data, and in clinical synthesis. Humans may always be superior at these tasks, although such a claim must be subjected to empirical testing from time to time.

What has been called the standard view of computer-assisted clinical diagnosis (Miller, 1990) holds in part that human cognitive processes, being more suited to the complex task of diagnosis than machine intelligence, should not be overridden or trumped by computers. The standard view states that when adequate (and even exemplary) decision-support tools are developed, they should be viewed and used as supplementary and subservient to human clinical judgment. They should take this role because the clinician caring for the patient knows and understands the patient's situation and can make compassionate judgments better than computer programs; they are also the individuals whom the state licenses, and specialty boards accredit, to practice medicine, surgery, nursing, pharmacy, or other health-related activities. Corollaries of the standard view are that: (1) practitioners have an obligation to use any computer-based tool responsibly, through adequate user training and by developing an understanding of the system's abilities and limitations; and (2) practitioners must not abrogate their clinical judgment reflexively when using computer-based decision aids. Because the skills required for diagnosis are in many respects different from those required for the acquisition, storage, and retrieval of laboratory data, there is no contradiction in urging extensive use of electronic laboratory information systems, but cautious or limited use (for the time being) of expert diagnostic decision-support tools.

The standard view addresses one aspect of the question, "How and when should computers be used in clinical practice?" by capturing important moral intuitions about error avoidance and evolving standards. Error avoidance and the benefits that follow from it shape the obligations of practitioners. In computer-software use, as in all other areas of clinical practice, good intentions alone may be insufficient to insulate recklessness from culpability. Thus, the standard view may be seen as a tool for both error avoidance and ethically optimized action.

Ethical software use should be evaluated against a broad background of evidence for actions that produce favorable outcomes. Because informatics is a science in extraordinary ferment, system improvements and evidence of such improvements are constantly emerging. Clinicians have an obligation to be familiar with this evidence after attaining minimal acceptable levels of familiarity with informatics in general and with the clinical systems they use in particular.

10.2.2 Appropriate Users and Educational Standards

Efficient and effective use of health care informatics systems requires training, experience, and education. Indeed, such requirements resemble those for other tools used in health care and in other domains. Inadequate preparation in the use of tools is an invitation to catastrophe. When the stakes are high and the domain large and complex—as is the case in the health professions—education and training take on moral significance.

Who should use a health care–related computer application? Consider expert decision-support systems as an example. An early paper on ethical issues in informatics noted that potential users of such systems include physicians, nurses, physicians' assistants, paramedical personnel, students of the health sciences, patients, and insurance and government evaluators (Miller et al., 1985). Are members of all these groups appropriate users? We cannot answer the question until we are clear about the precise intended use for the system (i.e., the exact clinical questions the system will address). The appropriate level of training must be correlated with the question at hand. At one end of an appropriate-use spectrum, we can posit that medical and nursing students should employ decision-support systems for educational purposes; this assertion is relatively free of controversy once it has been verified that such tools convey accurately a sufficient quantity and quality of educational content. But it is less clear that patients, administrators, or managed-care gatekeepers, for example, should use expert decision-support systems for assistance in making diagnoses, in selecting therapies, or in evaluating the appropriateness of health professionals' actions. To the extent that some systems present general medical advice in hypermedia format, such as might occur with Dr. Spock's print-based child care primer, use by laypersons may be condoned. There are additional legal concerns related to negligence and product liability, however, when health-related products are sold directly to patients rather than to licensed practitioners and when such products give patient-specific counsel rather than general clinical advice.

Suitable use of a software program that helps a user to suggest diagnoses, to select therapies, or to render prognoses must be plotted against an array of goals and best practices for achieving those goals, including consideration of the characteristics and requirements of individual patients. For example, the multiple interconnected inferential strategies required for arriving at an accurate diagnosis depend on knowledge of facts; experience with procedures; and familiarity with human behavior, motivation, and values. **Diagnosis** is a process rather than an event (Miller, 1990), so even well-validated diagnostic systems must be used appropriately in the overall context of patient care.

To use a diagnostic decision-support system, the clinician must be able to recognize when the computer program has erred, and, when it is accurate, what the output means and how it should be interpreted. This ability requires knowledge of both the diagnostic sciences and the software applications and their limitations. After

assigning a diagnostic label, the clinician must communicate the diagnosis, prognosis, and implications to a patient and must do so in ways both appropriate to the patient's educational background and conducive to future treatment goals. It is not enough to be able to tell patients that they have cancer, human immunodeficiency virus (HIV), diabetes, or heart disease and simply to hand over a number of prescriptions. The care provider must also offer context when available, comfort when needed, and hope as appropriate. The reason many jurisdictions require pretest and posttest HIV counseling, for instance, is not to vex busy health professionals but rather to ensure that comprehensive, high-quality care—rather than just diagnostic labeling—has been delivered.

This discussion points to the following set of ethical principles for appropriate use of decision-support systems:

1. A computer program should be used in clinical practice only after appropriate evaluation of its efficacy and the documentation that it performs its intended task at an acceptable cost in time and money.
2. Users of most clinical systems should be health professionals who are qualified to address the question at hand on the basis of their licensure, clinical training, and experience. Software systems should be used to augment or supplement, rather than to replace or supplant, such individuals' decision making.
3. All uses of informatics tools, especially in patient care, should be preceded by adequate training and instruction, which should include review of all available forms of previous product evaluations.

Such principles and claims should be thought of as analogous to other standards or rules in clinical medicine and nursing.

10.2.3 Obligations and Standards for System Developers and Maintainers

Users of clinical programs must rely on the work of other people who are often far removed from the context of use. Users depend on the developers and maintainers of a system and must trust evaluators who have validated a system for clinical use. Health care software applications are among the most complex tools in the technological armamentarium. Although this complexity imposes certain obligations on end users, it also commits a system's developers, designers, and maintainers to adhere to reasonable standards and, indeed, to acknowledge their moral responsibility for doing so.

Ethics, Standards, and Scientific Progress

The very idea of a **standard of care** embodies a number of complex assumptions linking ethics, evidence, outcomes, and professional training. To say that a nurse or physician must adhere to a standard is to say, in part, that they ought not to stray from procedures that have been shown or are generally believed to work better than other procedures. Whether a procedure or device "works better" than another can be difficult to determine. Such determinations in the health sciences constitute progress and

indicate that we know more than we used to know. Criteria for evidence and proof are applied. Evidence from randomized controlled trials is preferable to evidence from uncontrolled retrospective studies, and verification by independent investigators is required before the most recent reports are put into common practice.

People who develop, maintain, and sell health care computing systems and components have obligations that parallel those of system users. These obligations include holding patient care as the leading value. The Hippocratic injunction primum non nocere (first do no harm) applies to developers as well as to practitioners. Although this principle is easy to suggest and, generally, to defend it invites subtle, and sometimes overt, resistance from people who hold profit or fame as primary motivators. To be sure, quests for fame and fortune often produce good outcomes and improved care, at least eventually. Even so, that approach fails to take into account the role of intention as a moral criterion.

In medicine, nursing, and psychology, a number of models of the **professional–patient relationship** place trust and advocacy at the apex of a hierarchy of values. Such a stance cannot be maintained if goals and intentions other than patient well-being are (generally) assigned primacy. The same principles apply to people who produce and attend to health care information systems. Because these systems are health care systems—and are not devices for accounting, entertainment, real estate, and so on—and because the domain is shaped by pain, vulnerability, illness, and death, it is essential that the threads of trust run throughout the fabric of clinical system design and maintenance.

System purchasers, users, and patients must trust developers and maintainers to recognize the potentially grave consequences of errors or carelessness, trust them to care about the uses to which the systems will be put, and trust them to value the reduced suffering of other people at least as much as they value their own personal gain. We emphatically do not mean to suggest that system designers and maintainers are blameworthy or unethical if they hope and strive to profit from their diligence, creativity, and effort. Rather, we suggest that no amount of financial benefit for a designer can counterbalance bad outcomes or ill consequences that result from recklessness, avarice, or inattention to the needs of clinicians and their patients.

Quality standards should stimulate scientific progress and innovation while safeguarding against system error and abuse. These goals might seem incompatible, but they are not. Let us postulate a standard that requires timely updating and testing of knowledge bases that are used by decision-support systems. To the extent that database accuracy is needed to maximize the accuracy of inferential engines, it is trivially clear how such a standard will help to prevent decision-support mistakes. Furthermore, the standard should be seen to foster progress and innovation in the same way that any insistence on best possible accuracy helps to protect scientists and clinicians from pursuing false leads, or wasting time in testing poorly wrought hypotheses. It will not do for database maintainers to insist that they are busy doing the more productive or scientifically stimulating work of improving knowledge representation, say, or database design. Although such tasks are important, they do not supplant the tasks of updating and testing tools in their current configuration or structure. Put differently, scientific and technical standards are perfectly able to stimulate progress while taking a cautious or even conservative stance toward permissible risk in patient care.

This approach has been described as "progressive caution." "Medical informatics is, happily, here to stay, but users and society have extensive responsibilities to ensure that we use our tools appropriately. This might cause us to move more deliberately or slowly than some would like. Ethically speaking, that is just too bad" (Goodman, 1998b).

System Evaluation as an Ethical Imperative

Any move toward "best practices" in health informatics is shallow and feckless if it does not include a way to measure whether a system performs as intended. This and related measurements provide the ground for quality control and, as such, are the obligations of system developers, maintainers, users, administrators, and perhaps other players (see Chapter 11).

> Medical computing is not merely about medicine or computing. It is about the introduction of new tools into environments with established social norms and practices. The effects of computing systems in health care are subject to analysis not only of accuracy and performance but of acceptance by users, of consequences for social and professional interaction, and of the context of use. We suggest that system evaluation can illuminate social and ethical issues in medical computing, and in so doing improve patient care. That being the case, there is an ethical imperative for such evaluation. (Anderson and Aydin, 1998)

To give a flavor of how a comprehensive evaluation program can ethically optimize implementation and use of an informatics system, consider these ten criteria for system scrutiny (Anderson and Aydin, 1994):

1. Does the system work as designed?
2. Is it used as anticipated?
3. Does it produce the desired results?
4. Does it work better than the procedures it replaced?
5. Is it cost effective?
6. How well have individuals been trained to use it?
7. What are the anticipated long-term effects on how departments interact?
8. What are the long-term effects on the delivery of medical care?
9. Will the system have an impact on control in the organization?
10. To what extent do effects depend on practice setting?

Another way to look at this important point is that people use computer systems. Even the finest system might be misused, misunderstood, or mistakenly allowed to alter or erode previously productive human relationships. Evaluation of health information systems in their contexts of use should be taken as a moral imperative. Such evaluations require consideration of a broader conceptualization of "what works best" and must look toward improving the overall health care delivery system rather than only that system's technologically based components. These higher goals entail the creation of a corresponding mechanism for ensuring institutional oversight and responsibility (Miller and Gardner, 1997a, 1997b).

10.3 Privacy, Confidentiality, and Data Sharing

Some of the greatest challenges of the Information Age arise from placing computer applications in health care settings while upholding traditional principles. One challenge involves balancing two competing values: (1) free access to information, and (2) protection of patients' **privacy** and **confidentiality**.

Only computers can manage the vast amount of information generated during clinical encounters and other health care transactions; at least in principle, such information should be easily available to health professionals so that they can care for patients effectively. Yet, making this information readily available creates opportunities for access by extraneous individuals. Access may be available to curious health care workers who do not need the information to fulfill job-related responsibilities, and, even more worrisome, to other people who might use the information to harm patients physically, emotionally, or financially. Seemingly, clinical system administrators must therefore choose between either improving care through use of computer systems or protecting confidentiality by restricting use of computer systems. Fortunately, it is a mistake to view these objectives as incompatible.

10.3.1 Foundations of Health Privacy and Confidentiality

Privacy and confidentiality are necessary for people to mature as individuals, to form relationships, and to serve as functioning members of society. Imagine what would happen if the local newspaper produced a daily account detailing everyone's actions, meetings, and conversations. It is not that most people have terrible secrets to hide but rather that the concepts of solitude, intimacy, and the desire to be left alone make no sense without the expectation that our actions and words will be kept private and held in confidence.

The terms *privacy* and *confidentiality* are not synonymous. Privacy generally applies to people, including their desire not to suffer eavesdropping, whereas confidentiality is best applied to information. One way to think of the difference is as follows. If someone follows you and spies on you entering an acquired immunodeficiency syndrome (AIDS) clinic, your privacy is violated; if someone sneaks into the clinic and looks at your health care record, your record's confidentiality is breached. In discussions of the electronic health care record, the term privacy may also refer to individuals' desire to restrict the disclosure of personal data (National Research Council, 1997).

There are several important reasons to protect privacy and confidentiality. One is that privacy and confidentiality are widely regarded as *rights* of all people, and such protections help to accord them respect. On this account, people do not need to provide a justification for keeping their health data secret; privacy and confidentiality are entitlements that a person does not need to earn, to argue for, or to defend. Another reason is more practical: protecting privacy and confidentiality benefits both individuals and society. Patients who know that their health care data will not be shared inappropriately are more comfortable disclosing those data to clinicians. This trust is vital for the successful physician–patient or nurse–patient relationship, and it helps practitioners to do their jobs.

Privacy and confidentiality protections also benefit public health. People who fear disclosure of personal information are less likely to seek out professional assistance, increasing the risks that contagion will be spread and maladies will go untreated. In addition, and sadly, people still suffer discrimination, bias, and stigma when certain health data do fall into the wrong hands. Financial harm may occur if insurers are given unlimited access to family members' records, or access to patients' genetic-testing results, because some insurers might be tempted to increase the price of insurance for individuals at higher risk of illness.

The ancient idea that physicians should hold health care information in confidence is therefore applicable whether the data are written on paper, etched in stone, or embedded in silicon. The obligations to protect privacy and to keep confidences fall to system designers and maintainers, to administrators, and, ultimately, to the physicians, nurses, and other people who elicit the information in the first place. The upshot for all of them is this: protection of privacy and confidentiality is not an option, a favor, or a helping hand offered to patients with embarrassing health care problems; it is a duty that does not vary with the malady or the data-storage medium.

Some sound clinical practice and public-health traditions run counter to the idea of absolute confidentiality. When a patient is hospitalized, it is expected that all appropriate (and no inappropriate) employees of the institution—primary-care physicians, consultants, nurses, therapists, and technicians—will be given access to the patient's medical records, when it is in the interest of patient care to do so. In most communities of the United States, the contacts of patients who have active tuberculosis or certain sexually transmitted diseases are routinely identified so that they may receive proper medical attention; the public interest is protected because the likelihood is decreased that they will transmit an infection unknowingly to other people. In addition, it is essential for health care researchers to be able to pool data from patient cases that meet specified conditions to determine the natural history of the disease and the effects of various treatments. Examples of benefits from such pooled data analyses range from the ongoing results generated by regional collaborative chemotherapy trials to the discovery, more than two decades ago, of the appropriateness of shorter lengths of stay for patients with myocardial infarction (McNeer et al., 1975). Most recently, the need for robust **syndromic surveillance** has been asserted as necessary for adequate bioterrorism preparedness.

10.3.2 Electronic Clinical and Research Data

Access to electronic patient records holds extraordinary promise for clinicians and for other people who need timely, accurate patient data. Institutions that are not using computer-based patient records may be falling behind, a position that may eventually become blameworthy. On the other hand, systems that make it easy for clinicians to access data also make it easy for other people to access it. Failure to prevent inappropriate access is at least as wrong as failure to provide adequate and appropriate access. It might therefore seem that the computer-based patient record imposes contradictory burdens on system overseers and users.

In fact, there is no contradiction between the obligation to maintain a certain standard of care (in this case, regarding minimal levels of computer use) and ensuring that such a

technical standard does not imperil the rights of patients. Threats to confidentiality and privacy are fairly well known. They include economic abuses, or discrimination by third-party payers, employers, and others who take advantage of the burgeoning market in health data; insider abuse, or record snooping by hospital or clinic workers who are not directly involved in a patient's care but examine a record out of curiosity, for blackmail, and so on; and malevolent hackers, or people who, via networks or other means, copy, delete, or alter confidential information (National Research Council, 1997). Indeed, the National Research Council has noted problems arising from widespread dissemination of information throughout the health care system—dissemination that often occurs without explicit patient consent. Health care providers, third-party payers, managers of pharmaceutical benefits programs, equipment suppliers, and oversight organizations collect large amounts of patient-identifiable health information for use in managing care, conducting quality and utilization reviews, processing claims, combating fraud, and analyzing markets for health products and services (National Research Council, 1997).

The proper approach to such challenges is one that will ensure both that appropriate clinicians and other people have rapid, easy access to patient records and that other people do not have access. Is that another contradictory burden? No. There are several ways to restrict inappropriate access to electronic records. They are generally divided into technological methods and institutional or policy approaches (Alpert, 1998):

- Technological methods: Computers can provide the means for maximizing their own security, including authenticating users, by making sure that users are who they say they are; prohibiting people without a professional need from accessing health information; and using audit trails, or logs, of people who do inspect confidential records so that patients and other people can review the logs.
- Policy approaches: The National Research Council has recommended that hospitals and other health care organizations create security and confidentiality committees and establish education and training programs. These recommendations parallel an approach that has worked well elsewhere in hospitals for matters ranging from infection control to bioethics.

Such recommendations are all the more important when health data are accessible through networks. The rapid growth of **integrated delivery networks (IDNs)** (see Chapter 13) and the National Health Information Infrastructure (NHII), for example, illustrates the need not to view health data as a well into which one drops a bucket but rather as an irrigation system that makes its contents available over a broad—sometimes an *extremely* broad—area. It is not yet clear whether privacy and confidentiality protections that are appropriate in hospitals will be valid in a networked environment. System developers, users, and administrators are obliged to identify appropriate measures. There is no excuse for failing to make ethics a top priority throughout the data storage and sharing environment.

Electronic Data and Human Subjects Research

The use of patient information for **clinical research** and for quality assessment raises interesting ethical challenges. The presumption of a right to confidentiality seems to

include the idea that patient records are inextricably linked to patient names or to other identifying data. In an optimal environment, then, patients can monitor who is looking at their records. But if all unique identifiers have been stripped from the records, is there any sense in talking about confidentiality?

The benefits to **public health** loom large in considering record-based research. A valuable benefit of the electronic health care record is the ability to access vast numbers of patient records to determine the incidence and prevalence of various maladies, to track the efficacy of clinical interventions, and to plan efficient resource allocation (see Chapter 14). Such research and planning would, however, impose onerous or intractable burdens if informed, or valid consent had to be obtained from every patient whose record was represented in the sample. To cite confidentiality as an impediment to all such research is to stand on ceremony that not only fails to protect patients but also forecloses on potentially beneficial scientific investigations.

A more practical course is to establish safeguards that optimize the research ethically. This goal can be reached via a number of paths. The first is to establish mechanisms to anonymize the information in individual records or to decouple the data contained in the records from any unique patient identifier. This task is not always straightforward. A specific job description ("this 30-year-old starting quarterback of the Wildcats professional football team was admitted with a shattered collarbone"), or a rare disease diagnosis coupled with demographic data, or a nine-digit postal code may act as a surrogate unique identifier; that is, detailed information can serve as a data fingerprint that picks out an individual patient even though the patient's name, Social Security number, or other (official) unique identifier has been removed from the record.

Such challenges point to a second means of optimizing database research ethically, the use of institutional panels, such as **medical record committees** or institutional review boards. Submission of database research to appropriate institutional scrutiny is one way to make the best use of more or less anonymous electronic patient data. Competent panel members should be educated in the research potential of electronic health care records, as well as in ethical issues in epidemiology and public health. Scrutiny by such committees could also ethically optimize internal research for quality control, outcomes monitoring, and so on (Goodman, 1998b; Miller and Gardner, 1997a, 1997b).

Challenges in Bioinformatics

Safeguards are increasingly likely to be challenged as genetic information makes its way into the health care record (see Chapter 22). The risks of bias, discrimination, and social stigma increase dramatically as **genetic data** become available to clinicians and investigators. Indeed, genetic information "goes beyond the ordinary varieties of medical information in its predictive value" (Macklin, 1992). Genetic data also may be valuable to people predicting outcomes, allocating resources, and the like (Table 10.1). In addition, genetic data are rarely associated with only a single person; they may provide information about relatives, including relatives who do not want to know about their genetic makeup or maladies as well as relatives who would love dearly to know more about their kin's genome. There is still much work to be done in sorting out and addressing the

Table 10.1. Correlation of clinical findings with genetic data.[a]

Syndrome	Number of signs	Clinical findings
Atkin-Flaitz	3	Short stature, obesity, hypertelorism
Young-Hughes	2	Short stature, obesity
Vasquez	2	Short stature, obestity
Stoll	2	Short stature, obesity
Simpson-Golabi-Behemel	2	Obesity, hypertelorism
Otopalato-Digital	2	Short stature, hypertelorism
FG	2	Short stature, hypertelorism
Chudley	2	Short stature, obesity
Borjeson	2	Short stature, obesity
Albright Hereditary Osteodystrophy	2	Short stature, obesity
Aarskog	2	Short stature, hypertelorism

[a]Databases with genetic information can be used to help correlate clinical findings with diagnoses of genetic maladies. Here are the results of a "Make Diagnosis" query based on short stature, obesity, and hypertelorism (abnormally large distance between paired organs, especially eyes) performed on the X-Linked Recessive Mental Retardation Database at the University of Miami.
(*Source*: Division of Genetics, Department of Pediatrics, University of Miami School of Medicine.)

ethical issues related to electronic storage, sharing, and retrieval of genetic data (Goodman, 1996).

Bioinformatics offers excellent opportunities to increase our knowledge of genetics, genetic diseases, and public health. These opportunities, however, are accompanied by responsibilities to attend to the ethical issues raised by methods, applications, and consequences.

10.4 Social Challenges and Ethical Obligations

The expansion of **evidence-based medicine** and, in the United States, of managed care places a high premium on the tools of health informatics. The need for data on clinical outcomes is driven by a number of important social and scientific factors. Perhaps the most important among these factors is the increasing unwillingness of governments and insurers to pay for interventions and therapies that do not work or that do not work well enough to justify their cost.

Health informatics helps clinicians, administrators, third-party payers, governments, researchers, and other parties to collect, store, retrieve, analyze, and scrutinize vast amounts of data. Such tasks may be undertaken not for the sake of any individual patient but rather for cost analysis and review, quality assessment, scientific research, and so forth. These functions are important, and if computers can improve their quality or accuracy, then so much the better. Challenges arise when intelligent machines are mistaken for decision making surrogates or when institutional or public policy recommends or demands that computer output stand proxy for human cognition.

10.4.1 Informatics and Managed Care

Consider the extraordinary utility of **prognostic scoring systems** or machines that use physiologic and mortality data to compare new critical-care patients with thousands of previous patients (Knaus et al., 1991). Such systems allow hospitals to track the performance of their critical-care units by, say, comparing the previous year's outcomes to this year's or by comparing one hospital to another. If, for instance, patients with a particular profile tend to survive longer than their predecessors, then it might be inferred that **critical care** has improved. Such scoring systems can be useful for internal research and for quality management (Figure 10.1).

Now suppose that most previous patients with a particular physiologic profile have died in critical-care units; this information might be used to identify ways to improve care of such patients—or it might be used in support of arguments to contain costs by denying care to subsequent patients fitting the profile.

An argument in support of such a nonresearch application might be that decisions to withdraw or withhold care are often and customarily made on the basis of subjective and fragmented evidence; so it is preferable to make such decisions on the basis of objective data of the sort that otherwise underlie sound clinical practice. Such

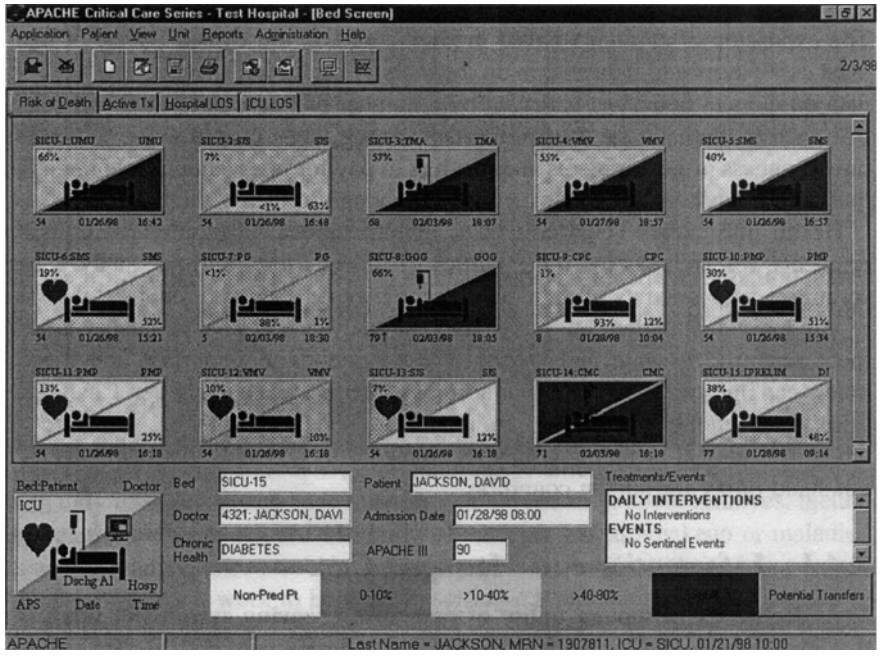

Figure 10.1. "Risk of Death" screen image from the APACHE III Critical Care Series. Using APACHE, clinicians in the intensive-care units are able to monitor critical events and required interventions, and administrators are able to manage the units' staffing based on the acuity of the patients on the units. (*Source*: Courtesy of APACHE Medical Systems, Inc.)

outcomes data are precisely what fuels the engines of managed care, wherein health professionals and institutions compete on the basis of cost and outcomes (see Chapter 23). Why, people may argue, should society, or a managed-care organization, or an insurance company pay for critical care when there is objective evidence that such care will not be efficacious? Contrarily, consider the effect of denying care to such patients on the basis of future scientific insights. Scientific progress is often made by noticing that certain patients do better under certain circumstances, and investigation of such phenomena leads to better treatments. If all patients meeting certain criteria were denied therapy on the basis of a predictive tool, it would become a self-fulfilling prophecy for a much longer time that all such patients would not do well.

Now consider use of a decision-support system to evaluate, review, or challenge decisions by human clinicians; indeed, imagine an insurance company using a diagnostic expert system to determine whether a physician should be reimbursed for a particular procedure. If the expert system has a track record for accuracy and reliability, and if the system "disagrees" with the human's diagnosis or treatment plan, then the insurance company can contend that reimbursement for the procedure would be a mistake. After all, why pay a provider for doing a procedure that is not indicated, at least according to the computer?

In the two examples just offered (a prognostic scoring system is used to justify termination of treatment to conserve resources, and a diagnostic expert system is used to deny a physician reimbursement for procedures deemed inappropriate), there seems to be justification for adhering to the computer output. There are, however, three reasons why it is problematic to use clinical computer programs to guide policy or practice in these ways:

1. As we saw earlier with the standard view of computational diagnosis (and, by easy extension, prognosis), human cognition is still superior to machine intelligence. The act of rendering a diagnosis or prognosis is not merely a statistical operation performed on uninterpreted data. Rather, identifying a malady and predicting its course requires understanding a complex ensemble of causal relations, interactions among a large number of variables, and having a store of salient background knowledge.
2. Decisions about whether to treat a given patient are often value laden and must be made relative to treatment goals. In other words, it might be that a treatment will improve the quality of life but not extend life, or vice versa (Youngner, 1988). Whether such treatment is appropriate cannot be determined scientifically or statistically (Brody, 1989).
3. Applying computational operations on aggregate data to individual patients runs the risk of including individuals in groups they resemble but to which they do not actually belong. Of course, human clinicians run this risk all the time—the challenge of inferring correctly that an individual is a member of a set, group, or class is one of the oldest problems in logic and in the philosophy of science. The point is that computers have not solved this problem, yet, and allowing policy to be guided by simple or unanalyzed correlations constitutes a conceptual error.

The idea is not that diagnostic or prognostic computers are always wrong—we know that they are not—but rather there are numerous instances in which we do not know

whether they are right. It is one thing to allow aggregate data to guide policy; doing so is just using scientific evidence to maximize good outcomes. But it is altogether different to require that a policy disallow individual **clinical judgment** and expertise.

Informatics can contribute in many ways to health care reform. Indeed, computer-based tools can help to illuminate ways to reduce costs, to optimize clinical outcomes, and to improve care. Scientific research, quality assessment, and the like are, for the most part, no longer possible without computers. But it does not follow that the insights from such research apply in all instances to the myriad variety of actual clinical cases at which competent human clinicians excel.

10.4.2 Effects of Informatics on Traditional Relationships

Patients are often sick, scared, and vulnerable. Treating illness, easing fear, and respecting vulnerability are among the core obligations of physicians and nurses. The growth of health informatics should be seen as posing exciting challenges to complement these traditional duties and the relationships that the duties govern. We have pointed out that medical decisions are shaped by nonscientific considerations. This point is important when we assess the effects of informatics on human relationships. Thus:

> The practice of medicine or nursing is not exclusively and clearly scientific, statistical, or procedural, and hence is not, so far, computationally tractable. This is not to make a hoary appeal to the "art and science" of medicine; it is to say that the science is in many contexts inadequate or inapplicable: Many clinical decisions are not exclusively medical—they have social, personal, ethical, psychological, financial, familial, legal, and other components; even art might play a role. (Miller and Goodman, 1998)

Professional–Patient Relationships

If computers, databases, and networks can improve physician–patient or nurse–patient relationships, perhaps by improving communication, then we shall have achieved a happy result. If reliance on computers impedes the abilities of health professionals to establish trust and to communicate compassionately, however, or further contributes to the dehumanization of patients (Shortliffe, 1994), then we may have paid too dearly for our use of these machines.

Suppose that a physician uses a decision-support system to test a diagnostic hypothesis or to generate differential diagnoses, and suppose further that a decision to order a particular test or treatment is based on that system's output. A physician who is not able to articulate the proper role of computational support in his decision to treat or test will risk alienating those patients who, for one reason or another, will be disappointed, angered, or confused by the use of computers in their care. To be sure, the physician might just withhold this information from patients, but such deception carries its own threats to trust in the relationship.

Patients are not completely ignorant about the processes that constitute human decision making. What they do understand, however, may be subverted when their doctors and nurses use machines to assist delicate cognitive functions. We must ask whether patients should be told the accuracy rate of decision machines—when they have yet to

be given comparable data for humans. Would such knowledge improve the informed-consent process, or would it "constitute another befuddling ratio that inspires doubt more than it informs rationality?" (Miller and Goodman, 1998).

To raise such questions is consistent with promoting the responsible use of computers in clinical practice. The question whether computer use will alienate patients is an empirical one; it is a question for which we have inadequate data to answer. (Do patients respond well to e-mail messages from their doctors, or do they not?) To address the question now anticipates potential future problems. We must ensure that the exciting potential of health informatics is not subverted by our forgetting that the practice of medicine, nursing, and allied professions is deeply human and fundamentally intimate and personal.

Consumer Health Informatics

The growth of the World Wide Web and the commensurate evolution of clinical and health resources on the Internet also raise issues for professional–patient relationships. **Consumer health informatics**—technologies focused on patients as the primary users—makes vast amounts of information available to patients. There is also, however, misinformation—even outright falsehoods and quackery—posted on some sites (see Chapter 14). If physicians and nurses have not established relationships based on trust, the erosive potential of apparently authoritative Internet resources can be great. Physicians accustomed to newspaper-inspired patient requests for drugs and treatments can expect everincreasing demands that are informed by Web browsing. The following issues will gain in ethical importance over the next decade:

- Peer review: How and by whom is the quality of a Web site to be evaluated? Who is responsible for the accuracy of information communicated to patients?
- Online consultations: There is yet no standard of care for online medical consultations. What risks do physicians and nurses run by giving advice to patients whom they have not met or examined? This question is especially important in the context of **telemedicine** or **remote-presence health care**, the use of video teleconferencing, image transmission, and other technologies that allow clinicians to evaluate and treat patients in other than face-to-face situations (see Chapter 24).
- Support groups: Internet support groups can provide succor and advice to the sick, but there is a chance that someone who might benefit from seeing a physician will not do so because of comforts and information otherwise attained, and that her not doing so will lead to bad consequences. How should this problem be addressed?

That a resource is touted as worthwhile does not mean that it is. We lack evidence to illuminate the utility of consumer health informatics and its effects on professional–patient relationships. Such resources should not be ignored, and they often are useful for improving health. But we insist that here—as with decision support, appropriate use and users, evaluation, and privacy and confidentiality—there is an ethical imperative to proceed with caution. Informatics, like other health technologies, will thrive if our enthusiasm is open to greater evidence and is wed to deep reflection on human values.

10.5 Legal and Regulatory Matters

The use of clinical computing systems in health care raises a number of legal and regulatory questions.

10.5.1 Difference Between Law and Ethics

As might be anticipated, ethical and legal issues often overlap. Ethical considerations apply in attempts to determine what is good or meritorious and which behaviors are desirable or correct in accordance with higher principles. Legal principles are generally derived from ethical ones but deal with the practical regulation of morality or behaviors and activities. Many legal principles deal with the inadequacies and imperfections in human nature and the less-than-ideal behaviors of individuals or groups. **Ethics** offers conceptual tools to evaluate and guide moral decision making. Laws directly tell us how to behave (or not to behave) under various specific circumstances and prescribe remedies or punishments for individuals who do not comply with the law. Historical precedent, matters of definition, issues related to detectability and enforceability, and evolution of new circumstances affect legal practices more than they influence ethical requirements.

10.5.2 Legal Issues in Health Care Informatics

Major legal issues related to the use of software applications in clinical practice and in biomedical research include liability under tort law; potential use of computer applications as expert witnesses in the courtroom; legislation governing privacy and confidentiality; and copyrights, patents, and intellectual property issues.

Liability Under Tort Law

In the United States and in many other nations, principles of tort law govern situations in which harm or injuries result from the manufacture and sale of goods and services (Miller et al., 1985). Because there are few, if any, U.S. legal precedents directly involving harm or injury to patients resulting from use of clinical software applications (as opposed to a small number of well-documented instances where software associated with medical devices has caused harm), the following discussion is hypothetical. The principles involved are, however, well established with voluminous legal precedents outside the realm of clinical software.

A key legal distinction is the difference between products and services. **Products** are physical objects, such as stethoscopes, that go through the processes of design, manufacture, distribution, sale, and subsequent use by purchasers. **Services** are intangible activities provided to consumers at a price by (presumably) qualified individuals.

The practice of clinical medicine has been deemed a service through well-established legal precedents. On the other hand, clinical software applications can be viewed as either goods (software programs designed, tested, debugged, placed on diskettes or other media, and distributed physically to purchasers) or services (applications that

provide advice to practitioners engaged in a service such as delivering health care). There are few legal precedents to determine unequivocally how software will be viewed by the courts, and it is possible that clinical software programs will be treated as goods under some circumstances and as services under others.

Two ideas from tort law potentially apply to the clinical use of software systems: (1) the **negligence theory**, and (2) **strict product liability**. Providers of goods and services are expected to uphold the standards of the community in producing goods and delivering services. When individuals suffer harm due to substandard goods or services, they may sue the service providers or goods manufacturers to recover damages. **Malpractice** litigation in health care is based on negligence theory.

Because the law views delivery of health care as a service (provided by clinicians), it is clear that negligence theory will provide the minimum legal standard for clinicians who use software during the delivery of care. Patients who are harmed by clinical practices based on imperfect software applications may sue the health care providers for negligence or malpractice, just as patients may sue attending physicians who rely on the imperfect advice of a human consultant (Miller et al., 1985). Similarly, a patient might sue a practitioner who has not used a decision-support system when it can be shown that use of the decision-support system is part of the current standard of care, and that use of the program might have prevented the clinical error that occurred (Miller, 1989). It is not clear whether the patients in such circumstances can also sue the software manufacturers, as it is the responsibility of the licensed practitioner, and not of the software vendor, to uphold the standard of care in the community through exercising sound clinical judgment. Based on a successful malpractice suit against a clinician who used a clinical software system, it might be possible for the practitioner to sue the manufacturer or vendor for negligence in manufacturing a defective clinical software product, but cases of this sort have not yet been filed. If there were such suits, it might be difficult for a court to discriminate between instances of improper use of a blameless system and proper use of a less than perfect system.

In contrast to negligence, strict product liability applies only to harm caused by defective products and is not applicable to services. The primary purpose of strict product liability is to compensate the injured parties rather than to deter or punish negligent individuals (Miller et al., 1985). For strict product liability to apply, three conditions must be met:

1. The product must be purchased and used by an individual.
2. The purchaser must suffer physical harm as a result of a design or manufacturing defect in the product.
3. The product must be shown in court to be "unreasonably dangerous" in a manner that is the demonstrable cause of the purchaser's injury.

Note that negligence theory allows for adverse outcomes. Even when care is delivered in a competent, caring, and compassionate manner, some patients with some illnesses will not do well. Negligence theory protects providers from being held responsible for all individuals who suffer bad outcomes. As long as the quality of care has met the standards, the practitioner should not be found liable in a malpractice case (Miller et al., 1985). Strict product liability, on the other hand, is not as forgiving or understanding.

No matter how good or exemplary are a manufacturer's designs and manufacturing processes, if even one in ten million products is defective, and that one product defect is the cause of a purchaser's injury, then the purchaser may collect damages (Miller et al., 1985). The plaintiff needs to show only that the product was unreasonably dangerous and that its defect led to harm. In that sense, the standard of care for strict product liability is 100 percent perfection. To some extent, appropriate product labeling (e.g., "Do not use this metal ladder near electrical wiring") may protect manufacturers in certain strict product liability suits in that clear, visible labeling may educate the purchaser to avoid "unreasonably dangerous" circumstances. Appropriate labeling standards may benefit users and manufacturers of clinical expert systems (Geissbuhler and Miller, 1997).

Health care programs sold to clinicians who use them as decision-support tools in their practices are likely to be treated under negligence theory as services. When advice-giving clinical programs are sold directly to patients, however, and there is less opportunity for intervention by a licensed practitioner, it is more likely that the courts will treat them as products, using strict product liability, because the purchaser of the program is more likely to be the individual who is injured if the product is defective.

Privacy and Confidentiality

The ethical basis for privacy and confidentiality in health care is discussed in Section 10.3.1. It is unfortunate that the legal state of affairs for privacy and confidentiality of electronic health records is at present chaotic (as it is for written records, to some extent). This state of affairs has not significantly changed in the three decades since it was described in a classic *New England Journal of Medicine* article (Curran et al., 1969).

However, a key U.S. law, the Health Insurance Portability and Accountability Act (HIPAA), became effective in 2002, prompting significant change—especially with the April 2003 application of the law's privacy standards. A major impetus for the law was that the process of "administrative simplification," prized for its potential to increase efficiency and reduce costs, would also pose threats to patient privacy and confidentiality. Coming against a backdrop of a variety of noteworthy cases in which patient data were improperly—and often embarrassingly—disclosed, the law was also seen as a badly needed tool to restore confidence in the ability of health professionals to protect confidentiality. While the law has been accompanied by debate both on the adequacy of its measures and the question whether compliance was unnecessarily burdensome, it nevertheless establishes the first nationwide privacy protections. At its core, it embodies the idea that individuals should control disclosure of their health data. Among its provisions, the law requires that patients be informed about their privacy rights; that uses of "protected health information" not needed for treatment, payment or operations be limited to exchanges of the "minimum necessary" amount of information; and that all employees in "covered entities" be educated about privacy (see Web sites by the U.S. Government, http://aspe.hhs.gov/admnsimp; Georgetown University, http://www.healthprivacy.org; or the University of Miami, http://privacy.med.miami.edu, for overviews).

Copyright, Patents, and Intellectual Property

Intellectual property protection afforded to developers of software programs, biomedical knowledge bases, and World Wide Web pages remains an underdeveloped area of law. Although there are long traditions of copyright and patent protections for nonelectronic media, their applicability to computer-based resources is not clear. **Copyright law** protects intellectual property from being copied verbatim, and **patents** protect specific methods of implementing or instantiating ideas. The number of lawsuits in which one company claimed that another copied the functionality of its copyrighted program (i.e., its "look and feel") has grown, however, and it is clear that copyright law does not protect the "look and feel" of a program beyond certain limits. Consider, for example, the unsuccessful suit in the 1980s by Apple Computer, Inc., against Microsoft, Inc., over the "look and feel" of Microsoft Windows as compared with the Apple Macintosh interface (which itself resembled the earlier Xerox Alto interface).

It is not straightforward to obtain copyright protection for a list that is a compilation of existing names, data, facts, or objects (e.g., the telephone directory of a city), unless you can argue that the result of compiling the compendium creates a unique object (e.g., a new organizational scheme for the information) (Tysyer, 1997). Even when the compilation is unique and copyrightable, the individual components, such as facts in a database, may not be copyrightable. That they are not copyrightable has implications for the ability of creators of biomedical databases to protect database content as intellectual property. How many individual, unprotected facts can someone copy from a copyright-protected database before legal protections prevent additional copying?

A related concern is the intellectual-property rights of the developers of materials made available through the World Wide Web. Usually, information made accessible to the public that does not contain copyright annotations is considered to be in the public domain. It is tempting to build from the work of other people in placing material on the Web, but copyright protections must be respected. Similarly, if you develop potentially copyrightable material, the act of placing it on the Web, in the public domain, would allow other people to treat your material as not protected by copyright. Resolution of this and related questions may await workable commercial models for electronic publication on the World Wide Web, whereby authors could be compensated fairly when other people use or access their materials. Electronic commerce should eventually provide copyright protection and revenue similar to the age-old models that now apply to paper-based print media; for instance, to use printed books and journals, you must generally borrow them from a library or purchase them.

10.5.3 Regulation and Monitoring of Computer Applications in Health Care

In 1996, the U.S. **Food and Drug Administration (FDA)** announced that it would hold public meetings to discuss new methods and approaches to regulating clinical software systems as medical devices. In response, a consortium of professional organizations related to health care information (the American Medical Informatics Association, the Center for Health Care Information Management, the Computer-Based Patient Record

Institute, the American Health Information Management Association, the Medical Library Association, the Association of Academic Health Science Libraries, and the American Nurses Association) drafted a position paper published in both summary format and as a longer discussion with detailed background and explanation (Miller and Gardner, 1997a, 1997b). The position paper was subsequently endorsed by the boards of directors of all the organizations (except the Center for Health Care Information Management) and by the American College of Physicians Board of Regents.

The recommendations from the consortium include these:

- Recognition of four categories of clinical system risks and four classes of monitoring and regulatory actions that can be applied based on the level of risk in a given setting.
- Local oversight of clinical software systems, whenever possible, through the creation of autonomous **software oversight committees**, in a manner partially analogous to the institutional review boards that are federally mandated to oversee protection of human subjects in biomedical research. Experience with prototypical software-oversight committees at pilot sites should be gained before any national dissemination.
- Adoption by health care-information system developers of a code of good business practices.
- Recognition that budgetary, logistic, and other constraints limit the type and number of systems that the FDA can regulate effectively.
- Concentration of FDA regulation on those systems posing highest clinical risk, with limited opportunities for competent human intervention, and FDA exemption of most other clinical software systems.

The recommendations for combined local and FDA monitoring are summarized in Table 10.2.

10.6 Summary and Conclusions

Ethical issues are important to health informatics. An initial ensemble of guiding principles, or ethical criteria, has emerged to orient decision making:

1. Specially trained humans remain, so far, best able to provide health care for other humans. Hence, computer software should not be allowed to overrule a human decision.
2. Practitioners who use informatics tools should be clinically qualified and adequately trained in using the software products.
3. The tools themselves should be carefully evaluated and validated.
4. Health informatics tools and applications should be evaluated not only in terms of performance, including efficacy, but also in terms of their influences on institutions, institutional cultures, and workplace social forces.
5. Ethical obligations should extend to system developers, maintainers, and supervisors as well as to clinician users.
6. Education programs and security measures should be considered essential for protecting confidentiality and privacy while improving appropriate access to personal patient information.

Table 10.2. Consortium recommendations for monitoring and regulating clinical software systems.[a]

Variable	Regulatory class			
	A	B	C	D
Supervision by FDA	Exempt from regulation	Excluded from regulation	Simple registration and postmarket surveillance required	Premarket approval and postmarket surveil lance required
	Optional	Mandatory	Mandatory	Mandatory
Role of software oversight committee	Monitor locally	Monitor locally instead of monitoring by FDA	Monitor locally and report problems to FDA as appropriate	Assure adequate local monitoring without replicating FDA activity
Software risk category				
1. Informational or generic systems[b]	All software in category	—	—	—
2. Patient-specific systems that provide low-risk assistance with clinical problems[c]	—	All software in category	—	—
3. Patient-specific systems that provide intermediate-risk support on clinical problems[d]	—	Locally developed or locally modified systems	Commercially developed systems that are not modified locally	—
4. High-risk, patient-specific systems[e]	—	Locally developed, noncommercial systems	—	Commercial systems

[a]FDA = Food and Drug Administration.
[b]Includes systems that provide factual content or simple, generic advice (such as "give flu vaccine to eligible patients in midautumn") and generic programs, such as spreadsheets and databases.
[c]Systems that give simple advice (such as suggesting alternative diagnoses or therapies without stating preferences), and give ample opportunity for users to ignore or override suggestions.
[d]Systems that have higher clinical risk (such as those that generate diagnoses or therapies ranked by score) but allow users to ignore or override suggestions easily; net risk is therefore intermediate.
[e]Systems that have great clinical risk and give users little or no opportunity to intervene (such as a closed-loop system that automatically regulates ventilator settings).
(*Source*: Miller R.A., Gardner R.M. (1997). Summary recommendations for responsible monitoring and regulation of clinical software systems. *Annals of Internal Medicine*, 127(9):842.)

7. Adequate oversight should be maintained to optimize ethical use of electronic patient information for scientific and institutional research.

New sciences and technologies always raise interesting and important ethical issues. Much the same is true for legal issues, although in the absence of precedent or legislation any legal analysis will remain vague. Similarly important challenges confront people who are trying to determine the appropriate role for government in regulating health care software. The lack of clear public policy for such software underscores the importance of ethical insight and education as the exciting new tools of health informatics become more common.

Suggested Readings

Goodman K.W. (Ed.) (1998). *Ethics, Computing, and Medicine: Informatics and the Transformation of Health Care*. Cambridge: Cambridge University Press.

This volume—the first devoted to the intersection of ethics and informatics—contains chapters on informatics and human values, responsibility for computer-based decisions, evaluation of medical information systems, confidentiality and privacy, decision support, outcomes research and prognostic scoring systems, and meta-analysis.

Miller R.A. (1990). Why the standard view is standard: People, not machines, understand patients' problems. *Journal of Medicine and Philosophy*, 15:581–591.

This contribution lays out the standard view of health informatics. This view holds, in part, that because only humans have the diverse skills necessary to practice medicine or nursing, machine intelligence should never override human clinicians.

Miller R.A., Schaffner K.F., Meisel, A. (1985). Ethical and legal issues related to the use of computer programs in clinical medicine. *Annals of Internal Medicine*, 102:529–536.

This article constitutes a major early effort to identify and address ethical issues in informatics. By emphasizing the questions of appropriate use, confidentiality, and validation, among others, it sets the stage for all subsequent work.

National Research Council (1997). *For the Record: Protecting Electronic Health Information*. Washington, D.C.: National Academy Press.

A major policy report, this document outlines leading challenges for privacy and confidentiality in medical information systems and makes several important recommendations for institutions and policymakers.

Questions for Discussion

1. What is meant by the standard view of appropriate use of medical information systems? Identify three key criteria for determining whether a particular use or user is appropriate.
2. Can quality standards for system developers and maintainers simultaneously safeguard against error and abuse and stimulate scientific progress? Explain your answers. Why is there an ethical obligation to adhere to a standard of care?

3. Identify (a) two major threats to patient confidentiality, and (b) policies or strategies that you propose for protecting confidentiality against these threats.
4. Many prognoses by humans are subjective and are based on faulty memory or incomplete knowledge of previous cases. What are the two drawbacks to using objective prognostic scoring systems to determine whether to allocate care to individual patients?
5. People who are educated about their illnesses tend to understand and to follow instructions, to ask insightful questions, and so on. How can the World Wide Web improve patient education? How, on the other hand, might Web access hurt traditional physician–patient and nurse–patient relationships?