The Practice of **Informatics**

JAMIA

Position Paper ■

Recommendations for Responsible Monitoring and Regulation of Clinical Software Systems

RANDOLPH A. MILLER, MD, REED M. GARDNER, PHD. For the American Medical Informatics Association (AMIA), the Computer-based Patient Record Institute (CPRI), the Medical Library Association (MLA), the Association of Academic Health Science Libraries (AAHSL), the American Health Information Management Association (AHIMA), and the American Nurses Association

A b s t r a c t   In mid-1996, the FDA called for discussions on regulation of clinical software programs as medical devices. In response, a consortium of organizations dedicated to improving health care through information technology has developed recommendations for the responsible regulation and monitoring of clinical software systems by users, vendors, and regulatory agencies. Organizations assisting in development of recommendations, or endorsing the consortium position include the American Medical Informatics Association, the Computer-based Patient Record Institute, the Medical Library Association, the Association of Academic Health Sciences Libraries, the American Health Information Management Association, the American Nurses Association, the Center for Healthcare Information Management, and the American College of Physicians. The consortium proposes four categories of clinical system risks and four classes of measured monitoring and regulatory actions that can be applied strategically based on the level of risk in a given setting. The consortium recommends local oversight of clinical software systems, and adoption by healthcare information system developers of a code of good business practices. Budgetary and other constraints limit the type and number of systems that the FDA can regulate effectively. FDA regulation should exempt most clinical software systems and focus on those systems posing highest clinical risk, with limited opportunities for competent human intervention.

■ **J Am Med Inform Assoc.** 1997;4:442–457.

Health care practitioners, clinical facilities, industry, and regulatory agencies share an obligation to manage clinical software systems responsibly, using a common, equitable framework. In mid-1996, the United States Food and Drug Administration (FDA) called for new discussions on the regulation of stand-

alone software programs as medical devices.[1,2] In response, a consortium of health information-related organizations has developed recommendations for public and private actions to accomplish responsible monitoring and regulation of clinical software systems.

The consortium believes that implementation of any new procedures for regulation of clinical software systems as medical devices requires detailed prior analysis of regulatory relevance to, or impact on, clinical software vendors, health care providers, and patients. Failure to carry out analyses prior to regulatory actions could halt progress in an emerging new industry that has substantial potential to improve the quality of health care delivery. Manufacturers, users, and patients cannot tolerate the delays in critical software improvements that might result from excessive governmental review and approval processes.

All parties (including the FDA, consortium members, and organizations endorsing the consortium position) emphasize the same objectives—protection and safety of patients, and facilitation of approaches that improve health care delivery and outcomes.

The authors, in consultation with the Editors of *JAMIA* and the *Annals of Internal Medicine*, have prepared a condensed version of this manuscript, more suitable for a clinical audience, for concurrent publication in the *Annals of Internal Medicine* (Miller RA, Gardner RM, American Medical Informatics Association, et al. Summary Recommendations for the Responsible Monitoring and Regulation of Clinical Software Systems. Forthcoming, Ann Intern Med, Vol. 127, November 1997.)

Background

Benefits of Clinical Software Systems

Clinical software systems are defined here as individual computer application programs, or interconnected groups of such programs, that are directly used in providing health care. Clinical software systems require supportive environments, including computer operating systems and network interfaces. A growing literature documents how clinical software systems can improve health care delivery processes and outcomes.[4-43] Users employ such systems to track and manage patient-related information, to retrieve local and general clinical information, and to apply clinical knowledge in making patient-specific decisions. Clinical system usage encompasses hospital information systems and electronic record-keeping[4-11]; clinical data repositories[12-13]; health service-specific support (e.g., laboratory, pharmacy, and dietary systems); decision support for diagnosis, therapy, or progno-

sis[14-26]; guidelines and reminders[27-38]; protocol management[39-40]; telecommunication and tele-health[41]; signal processing (e.g., ECG interpretation systems)[42]; image storage and analysis (e.g., picture archival and communications systems—PACS)[43]; advice-giving systems for patients; and other health-related applications.

To maximize benefit, providers should integrate significant technological advances promptly and safely into clinical practice. Currently, there are no widely accepted, practical standards for the evaluation, use, and monitoring of clinical software systems. The FDA is only beginning to formulate a definitive policy with respect to such systems. In our opinion, regulation and oversight of clinical systems is both too important and too complicated to be the sole responsibility of users, vendors, or regulatory agencies—a combined approach is required, with roles for each category of participants.

Obstacles to Evaluation and Monitoring of Clinical Software Systems

Determination of the safety of clinical software systems is difficult because of the varied nature of clinical software, the changes that occur when a software product is integrated into a complex clinical information management infrastructure, the changes to systems that occur during maintenance, and the miscellaneous interactions between software programs and their users.

Evaluation of Simple "Turnkey" Clinical Applications

It is difficult to evaluate and monitor even simple independent, turnkey programs—single software products that do not connect to or depend upon other application programs (other than an operating system). Such programs are often used "as is" on microcomputers in individual practitioners' offices, and only modified when users upgrade to the next version. According to a recent survey, individual clinical vendor products number at least several thousand.[45] In addition, there exist thousands of health-related, Internet-based World Wide Web resources of variable quality.

Persons evaluating the performance of a clinical software system employ numerous criteria in determining whether a system merits purchase, installation, continued utilization, or approval by a regulatory agency.[46-52] The appropriateness of a given evaluation method varies with the stage of system development.[47] While it is important during system development to evaluate system performance in isolated, artificially controlled situations, evaluators of more mature systems should compare clinicians caring for actual patients using the software to clinicians with-

out access—and not simply report "system performance" on a series of cases.

With respect to patient safety, approval of any system's performance should be based on demonstration of either absolute or relative benefit. For absolute benefit, system use should cause no measurable harm, produce outcomes at least as good as the status quo, and do so at an acceptable cost in time and money. For relative benefit, system use should demonstrate net improvement over the status quo—i.e., the system will reduce the overall level of patient morbidity, mortality, or costs, even though the system itself may cause adverse effects. For example, electrocardiogram (EKG) interpretation programs have acceptable relative benefit in patient care settings because they improve upon many physicians' ability to rapidly and effectively interpret EKGs, even though it is widely known that they are not as authoritative as expert Cardiologists, and may on occasion mislead health care providers.

Evaluation and Monitoring of Complex, Interconnected Clinical Software Systems

A software product may work well in isolation but fail when integrated with other software products or with unsupported network interfaces. Large clinical sites (such as tertiary referral centers) contain diverse hardware platforms, multiple networks, and many vendors' software products. Clement J. McDonald recently estimated that large U.S. health centers interconnect several dozen major clinical software systems, consisting of both vendors' clinical software products and locally developed software programs.[44] A diagram of the HELP System, developed at LDS Hospital in Salt Lake City, Utah,[6] illustrates how complex such systems can become (Fig. 1). Suppose, for example, that a small to medium-sized health care institution decides to purchase and connect via a network a series of applications for their laboratory, pharmacy, admission/discharge/transfer (ADT), dietary, and clerical order processing activities. If the institution considers ten different vendors that produce products of the sort being considered, there are 100,000 different basic configurations possible. Major referral centers install dozens of individual software components, each selected from more than a hundred possible product configurations (Fig. 1). One hundred choices for each of 12 components yields a trillion trillion (10^{24}) possible overall configurations for each large site! Because each clinical site combines different software products in different combinations, a universal evaluation of whether or not a given product will function safely when embedded in a clinical environment is impractical.

Evaluation of Clinical Software Systems that Change Over Time

A clinical application categorized as "safe and effective" based on extensive testing at its inception might become less than effective over time due to improper or inadequate maintenance. Both system software code and the clinical data supporting system functions may be altered in a manner that invalidates evaluation results for previous baseline products. Configuration and integration of complex systems requires testing, tuning, correction of software errors, modifications based on installation environments and user feedback, and upgrades, all of which increase local variability over time. These changes occur on an almost daily basis. Requiring a formal evaluation of safety or efficacy related to each system change would paralyze ongoing implementation.

Users: An Important Consideration in Evaluation and Monitoring

Clinical software users include institutions, individual health care providers, and the general public, including patients. In analyzing causes of system-related adverse events, it is essential to consider end-user factors.[46–52] Systems with exemplary hardware and software components can cause problems when users do not understand system applicability and limitations; when users do not understand how to input critical information into the system, when users cannot reliably interpret system output; or when it is difficult to integrate system use into common workflow patterns. Monitoring to detect problems often requires aggregation of objective observations from a number of sources and a perspective that goes beyond individual system components. Hence, "raw" complaints from individual users need to be analyzed to determine if the problem is in the software or in the user education program.

Past and Current FDA Regulation of Clinical Software Systems

Through its mandate from Congress to safeguard the public, the FDA has regulated marketing and use of medical devices. Section 201(h) of the 1976 Federal Food, Drug, and Cosmetic Act defines a medical device as any "instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease . . . or intended to affect the structure or any function of the body."[53] The FDA asserts that all clinical software programs, whether associated with biomedical

devices or stand-alone, are "contrivances," and therefore fall within the FDA's realm of responsibility for regulating medical devices.

The FDA regulates medical devices that are: (a) commercial products used in patient care; (b) devices used in the preparation or distribution of clinical biological materials (such as blood products); or (c) experimental devices used in research involving human subjects. Commercial vendors of specified types of medical devices must register as manufacturers with the FDA and list their devices as products with the FDA. Upon listing, FDA classifies medical devices by categories. In its regulation of classified medical devices, the FDA usually takes one of three courses of action. First, the FDA can "exempt" specific devices, or categories of devices, deemed to pose little or no risk. Second, the FDA employs the so-called 510(k) process—pre-market notification—for non-exempt systems. Through the 510(k) process, manufacturers attempt to demonstrate that their devices are equivalent, in purpose and function, to low-risk (FDA Class I or Class II) devices previously approved by FDA (or to devices marketed before 1976). Such devices can be cleared by FDA directly. Finally, the FDA requires pre-market approval (PMA) for higher-risk (FDA Class III) products and for products with new (unclassified) designs invented after 1976. Through the pre-market approval process, a manufacturer provides evidence to the FDA that a product performs its stated functions safely and effectively. Evidence for PMAs usually is presented in the form of controlled trials. Pre-market approval is especially important for those products which pose significant potential clinical risk. Exemption can take place in two ways: a device can be exempt from registration, and thus not subject to 510(k) requirements; or, a category of listed (classified) devices may be specifically exempted from certain regulatory requirements. Whenever a non-exempt product is modified substantially (as defined by FDA guidelines), the vendor must re-apply to the FDA for new clearance through the 510(k) or PMA mechanisms. The processes of 510(k) pre-market notification and pre-market approval typically take a few to many months to complete, and may involve numerous exchanges and iterations.

The FDA has a long history of regulating hardware medical devices, making it important to distinguish between medical device-associated software and other clinical software. Clinical software can be categorized as "stand-alone"—external to and independent of a medical hardware device—or "embedded"—an integral component of a medical hardware device. Of note, a second connotation of "stand-alone" system
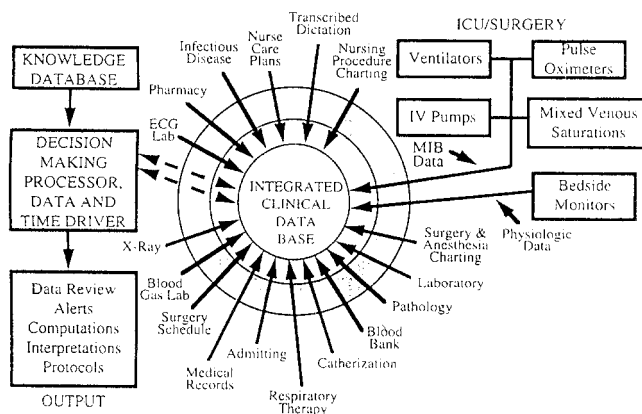
Figure 1 Diagram of HELP Information System at LDS Hospital, Salt Lake City, Utah.[6]

—a single, independent "turnkey" system—was previously discussed. However, in the context of FDA discussions, "stand-alone" refers to independence from a traditional (hardware) medical device. Embedded software is often placed on a computer ROM (read-only-memory) chip that physically controls all or part of a hardware medical device, such as a laboratory auto-analyzer or a cardiac pacemaker. The FDA regulates any embedded software program as part of the medical hardware device itself.

In general, the FDA does not actively regulate locally developed stand-alone software programs, whether developed by an individual or an institution, unless special circumstances apply. One such circumstance is local preparation of FDA-regulated biomaterials, such as blood products. The FDA regulates individual stand-alone software products that are commercially marketed by individual manufacturers. It rarely specifies or controls how independent vendors' products can be combined at a specific site, unless such products are components of a single, larger system, such as a PACS system. This is similar to FDA regulation of commercial pharmaceuticals, wherein the FDA regulates each individual drug comprising a chemotherapy protocol, but does not regulate multiple drug chemotherapy protocols themselves. The requirements for re-review are somewhat controversial, in that upgrading the network operating system of a component part of an FDA-regulated PACS system from version 3.1 to version 4.0 could potentially be viewed by the FDA as requiring resubmission for 510(k) or PMA approval. For this reason, the FDA has drafted and periodically updated guidelines on when to submit for re-approval.

In 1986, Frank Young, then director of the FDA, proposed a commendable plan for the oversight and regulation of clinical software.[54] This plan evolved into a

1989 draft FDA policy statement that was never formally adopted. That draft policy has served, until recently, as the basis for the FDA's actions with respect to stand-alone software systems. The 1989 draft policy recommended that the FDA exempt from regulation both information-providing educational systems and systems that generate patient-related advice for clinicians in a manner that licensed practitioners (users) could easily override. During the 1990s, the FDA has developed new draft regulations and guidelines for blood bank software systems[55,56] and for PACS systems.[57] The FDA is developing new guidelines for telemedicine systems as well.[58]

At present, aspects of FDA regulation of clinical software systems can be applied in an arbitrary manner. Although the FDA can initiate review of software products brought to its attention, for the most part, the agency depends on vendors to submit their products voluntarily both for initial review, and review after modifications. The review process itself may vary, because the FDA often employs a variety of different evaluators and consultants in reviewing similar products. Some vendors may be more likely than others to consider their software products as requiring FDA review.

3 Participating Organizations and Consensus Process

Participating Organizations

The American Medical Informatics Association (AMIA) is a non-profit organization dedicated to improving health care through the application of information technology. The more than 3,700 members of AMIA represent professions associated with healthcare informatics—physicians, nurses, biomedical engineers, computer scientists, information scientists, programmer-analysts, librarians, biomedical educators, biomedical researchers, vendor-consultants, dentists, veterinarians, students, and a variety of other health care practitioners. AMIA's goals are to promote the development of health care informatics as a recognized academic and professional discipline; to help solve health care problems through informatics research and development; and to promote diffusion of knowledge in the discipline of health care informatics. The Computer-based Patient Record Institute (CPRI) is a non-profit membership organization committed to advancing improvements in health care quality, cost and access through routine use of information technology. CPRI serves as a neutral forum for bringing the diverse interests of all health care stakeholders to-gether to develop common solutions. The Medical Library Association (MLA) is a professional organization representing approximately 5,000 individuals and institutions involved in the management and dissemination of biomedical information to support patient care, education, and research. MLA members serve society by developing new health information delivery systems, fostering educational and research programs for health sciences information professionals, and encouraging an enhanced public awareness of health care issues. The Association of Academic Health Sciences Libraries (AAHSL) is composed of the directors of libraries of 142 accredited U.S. and Canadian medical schools. AAHSL's goals are to promote excellence in academic health sciences libraries and to ensure that the next generation of health practitioners is trained in information-seeking skills that enhance the quality of health care delivery. The American Health Information Management Association (AHIMA) is the professional organization of more than 37,000 specialists in securing, analyzing, and managing patient records and health information. AHIMA members support quality patient care through advancing data accuracy, advocating confidentiality, and championing new information management technology. AHIMA, founded in 1928, accredits educational programs at 250 colleges and universities and is the certifying agency for health information managers and technicians. The American Nurses Association (ANA) is the only full-service professional organization representing the nation's 2.5 million Registered Nurses through its 53 constituent associations. ANA advances the nursing profession by fostering high standards of nursing practice, promoting the economic and general welfare of nurses in the workplace, projecting a positive and realistic view of nursing, and by lobbying the Congress and regulatory agencies on health care issues affecting nurses and the public. ANA has been involved in healthcare informatics since the early 1970s and continues to actively engage in diverse informatics activities. The American College of Physicians (ACP) was founded in 1915 to uphold the highest standards in medical education, practice, and research. Today, the College is the largest medical specialty society in the world. It has more than 100,000 members, including medical students as well as practicing physicians, and it is the only society of internists dedicated to providing education resources and information resources to the entire field of internal medicine as well as its subspecialties. The Center for Healthcare Information Management (CHIM) is a national, 100-plus member association for companies supplying information technology products and services to the healthcare industry—including software suppliers, consultants, hardware firms, network integrators, medical imaging companies, publishers, and

executive recruiters. CHIM members seek to bring a greater understanding and awareness among health-care professionals as to how information technology can be harnessed to improve the quality and cost-effectiveness of patient care.

Consensus Process

In an attempt to develop a parsimonious approach to handling proposals for changed regulations, the FDA has conducted, during 1996 and 1997, a series of public meetings that have included leaders from the information technology and health care arenas, representative professional organizations, and vendors. The first draft of the consensus recommendations was prepared as a discussion document by authors RAM and RMG, as representatives of the American Medical Informatics Association (AMIA) at the first (and subsequent) public meetings held by the FDA. Key contributions to the evolving position paper were then made by other members of the AMIA Public Policy Committee and the AMIA Board of Directors. After initial endorsement by the AMIA Board of Directors, subsequent suggestions and further revisions were contributed by the Center for Healthcare Information Management (CHIM); the Computer-based Patient Record Institute (CPRI), the Medical Library Association, the Association of Academic Health Sciences Libraries (AAHSL), the American Health Information Management Association (AHIMA), and the American Nurses Association (ANA). The Boards of Directors (or Regents) of the following not-for-profit organizations have now endorsed the recommendations entailed in this document: the American Medical Informatics Association (AMIA), the Computer-based Patient Record Institute (CPRI), the Medical Library Association (MLA), the Association of Academic Health Sciences Libraries (AAHSL), the American Health Information Management Association (AHIMA), the American Nurses Association (ANA), and the American College of Physicians (ACP). The Center for Healthcare Information Management (CHIM) has reviewed successive drafts of this document and contributed to its writing.

CHIM is supportive of the consortium's position, and holds the same opinions expressed in this document in all areas except for the definitions for proposed risk categories of clinical software systems and classes of regulations. The Appendix presents an algorithm prepared by CHIM suggesting how the FDA might review stand-alone clinical software systems for regulatory purposes. It should be noted that, while CHIM includes in its membership a number of commercial vendors from the healthcare information industry, the viewpoints of individual members have not been represented in this consensus document, and the original and subsequent drafts of the consortium's recommendations have been prepared and endorsed by not-for-profit organizations.

Consortium Recommendations

The consortium recommends that users, vendors, and regulatory agencies (including the FDA) adopt the guidelines detailed below. Detailed explanations and justifications follow in the section after the recommendations themselves. The recommendations go beyond the scope of interventions that the FDA or other vendor groups would ordinarily undertake, since they include clinical software products that are locally developed, shareware, non-commercial, and commercial.

Recommendation 1: We propose four categories of clinical software system risks and four classes of measured regulatory actions as a template for clinical facilities, vendors, and regulatory agencies to use in determining how to monitor or regulate any given clinical software system (Tables 1A and 1B).

Recommendation 2: We recommend local oversight of clinical software systems whenever possible, through creation of Software Oversight Committees, or "SOCs" (Tables 2A through 2D).

Recommendation 3: Budgetary and other constraints limit the type and number of systems that the FDA can regulate effectively. We recommend that the FDA focus its regulatory efforts on those systems posing highest clinical risk that give limited opportunities for competent human intervention (Tables 2A–2D). The majority of clinical software systems should be exempt from FDA regulation. The FDA should require producers of exempt clinical software systems to list them as products with the FDA for simple monitoring purposes—i.e., without having to undergo the 510(k) or PMA processes. The FDA should develop new, comprehensive standards for product labeling that are appropriate for clinical software products. The FDA should require manufacturers of most exempt and all non-exempt software products to adhere to labeling standards (Tables 2A–2D).

Recommendation 4: We recommend adoption by health care information system vendors and local software producers of a code of good business practices. The practices should include (but not be limited to) guidelines for quality manufacturing processes; standardized, detailed product labeling; responsible approaches to customer support; and, adoption of industry-wide standards for electronic information handling and sharing—including standards for health care information format, content, and transport.

Recommendation 5: We recommend that health information-related organizations work together with

Table 1A ■

Consortium Recommendations for Risk-based Categories of Clinical Software Systems

Category	Description	Category	Description
0	Informational or generic systems that provide factual content (electronic textbooks); verifiably calculate (showing all parameters used) simple quantities, such as drug dosage based on body weight; or give simple, straightforward advice based on user-reviewed guidelines (e.g., "give potassium supplementation to patients receiving digoxin who are hypokalemic"). Includes "content-free" generic software such as general database programs, generic spreadsheet programs. Non-clinical systems also fall in this category.		provide easy opportunities for practitioners to ignore or override them. For example, systems in this category might recommend a single patient-specific therapy over a number of alternative forms of therapy; recommend that the practitioner commit to (conclude) a specific diagnosis from a patient-specific differential diagnosis; or guide patients in determining which advanced-care directives might be appropriate for their situation. Systems in this category might also store and transmit patient-specific instructions for life-critical care (e.g., ventilator management or chemotherapy orders) to practitioners in a manner that is easily verified.
1	Low-risk, patient-specific systems that perform complex health-related functions with relatively low clinical risk and provide ample opportunities for practitioners to ignore or override them. Such systems might non-judgmentally suggest a number of alternative forms of therapy; list a comprehensive patient-specific differential diagnosis without making a conclusion; or provide an estimate of the patient's prognosis based on matched cases from a clinical database. Systems in this category might also store and transmit patient-specific "passive" data (e.g., laboratory results or clinical reports) in a manner that is easily verified.	3	High-risk, patient-specific systems that provide complex, health-related functions that have high clinical impact and provide little if any opportunity for practitioners to intervene in their function or to override them. For example, systems in this category might include individualized chemotherapy mixing and dispensing systems, systems that autonomously plan courses of radiation therapy for uploading into automated equipment to deliver the therapy, and systems that monitor physiological parameters and automatically adjust settings related to therapy (for example, a ventilator "auto-pilot").
2	Intermediate-risk, patient-specific systems that provide complex, health-related functions that have relatively high clinical risk, but		

other groups, including clinical professional associations, vendor organizations, regulatory agencies, and user communities, to advance our understanding and knowledge of approaches to regulating and monitoring clinical software systems.

Explanation and Justification for Consortium Recommendations

Explanation of Recommendation 1: Risk and Regulatory Categories

Software installation and maintenance must be treated as a process, not a single event. Review of a software environment at one point in time does not guarantee safety or efficiency at a later point in time. Decisions about whether to install and how to monitor clinical software systems should take into account: (a) the clinical risks posed by software malfunction or mis-use; (b) the extent of system autonomy from user oversight and control—the inability for qualified users, such as licensed practitioners, to recognize and easily override clinically inappropriate recommendations (or other forms of substandard software performance); (c) the pattern of distribution and degree of support for the software system, including local customization; (d) the complexity and variety of clinical software environments at installation sites; (e) evolution of systems and their environments over time; and, (f) the ability of proposed monitors or regulators to detect and correct problems in a timely manner that protects patients. The ability of licensed clinician-users to override a system should be a consideration for decreased regulatory intervention. It is important to identify the most logical forum for system oversight. The best choice will often be local monitoring through SOCs (as described below), rather than nationally centralized data collection and monitoring.

Table 1B ■

Consortium Recommendations for Regulatory Classes

Class	Description	Recommendation
A	Exempt from FDA regulation; local SOC monitoring optional	Good business practices would be applied by developers, vendors, and users.
B	Exempt from FDA regulation; local SOC monitoring mandatory	Commercial products in this category should adhere to product labeling standards, and commercial vendors should list products with FDA for simple identification purposes (no FDA review required). Good business practices recommended. Standardized surveys of isolated users could be conducted on request by the FDA (or FDA-approved regional organizations) for individuals who lack resources or expertise to implement local monitoring and review guidelines. The FDA would serve as a consultant to manufacturers, vendors, and SOC committees, rather than as a regulator.
C	Simplified, expedited initial FDA approval through verification that product labeling is accurate and adheres to standards; mandatory listing of products with FDA for post-marketing surveillance; application of usual FDA 510(k) or PMA processes to any products generKating concerns during post-marketing surveillance; local SOC monitoring mandatory.	Good business practices required. Reporting and recording of adverse events required with FDA collating and aggregating standardized reports after local collection and verification. FDA can require vendors with unusually large number of unexplained adverse event reports to undergo 510(k) or PMA to document safety and efficacy. In such trials, FDA should employ standard that the system demonstrates absolute or relative benefit (as defined above). Vendors required to maintain lists of users of each version of each system in this class.
D	Usual FDA 510(k) or PMA processes applied prior to marketing; local SOC monitoring mandatory.	Prior to marketing, vendors must submit to FDA evidence that system safely and efficaciously performs its stated functions. Good business practices required. Vendors must maintain lists of users of each version. Recording of adverse events required locally and reported to FDA using standardized forms for aggregation of data. Troubleshooting activities aggregated locally and reported after filtering to FDA. FDA may require additional testing if the rate of adverse events is too high.

We have proposed categories of clinical software systems based on patient risk and classes of regulatory interventions, as detailed in Tables 1A and 1B. Tables 2A through 2D represent our recommendations on how to apply the classes of regulatory actions responsibly to all clinical systems, based on the systems' risk categories. The recommendations in Tables 2A through 2D cannot be carried out solely by the FDA or by local institutions, vendors, or users. A combined approach with shared responsibilities is required. The consortium recommendations represent such an approach.

Explanation of Recommendation 2: Local Monitoring of Clinical Software Systems

Local software installation sites have the greatest ability to detect software problems, analyze their impact, and develop timely solutions. It would be advantageous to develop a program of institutional- and ven-

dor-level controls for the majority of clinical software products, rather than to mandate comprehensive, cumbersome, inefficient, and costly national-level monitoring.

Institutional Review Boards (IRBs) provide an example of a local monitoring process that is in widespread use.[59–61] In order to protect the human subjects of research, federal law has required each clinical facility engaged in patient research have an IRB to review, approve, and monitor research protocols locally. Each IRB includes clinical experts, administrators, individuals familiar with research study designs and methods, and persons experienced in data analysis. Some IRBs also include laypersons as representatives of the patient community. The IRBs review the purpose of proposed research; the anticipated benefits to individuals and to the general community; the risks to subjects in terms of health outcomes, pain and suffering, and expenses; informed consent, voluntary participa-

Table 2A ◼

Proposed Classes of Clinical Software Exemptions and Regulation by Category of Software

Type of Software	Description
Class A	Software exempt from FDA regulation; local SOC monitoring optional. (Please refer to definitions of risk categories and regulatory classes in Table 1.)
Category 0	Informational or generic products
Category 0	Non-clinical systems
	Any system not directly involved in patient care and any system not serving as an integral component of a larger system providing patient care—i.e., systems that do not play any role in suggesting diagnoses, suggesting prognoses, or suggesting or implementing orders or treatments.

tion, and ability to withdraw from the research study; and the plans for monitoring and conduct of the research protocol itself—e.g., ability to detect adverse outcomes or grossly positive benefits so that the study can be terminated early, if indicated. In making decisions, the locally autonomous IRBs can take regional demographics, local practice patterns, patient concerns, and individual researchers' skills and past records into account much more efficiently and effectively than could a centralized national agency.

While IRBs per se are not well qualified to review and monitor clinical software systems, they provide a model for creating a multidisciplinary team with appropriate expertise at the local level. Local and regional Software Oversight Committees (SOCs) could enlist members with expertise in health care informatics, clinical practice, data quality, biomedical ethics, patients' perspectives, and quality improvement. When the complexity, diversity, and number of clinical software and computer hardware products at an installation site reach a critical size, a local SOC should be formed to review clinical software on an ongoing basis within the institution. On a similar note, the Joint Council for the Accreditation of Healthcare Organizations (JCAHO) reviews organizations' systems and processes for improving their performance, and specifically includes information management as one of the areas reviewed. Small practitioners' offices or smaller community hospitals without adequate expertise could participate in regional SOCs, or possibly request consultations from local SOCs at larger institutions.

The SOCs would develop and follow guidelines for local or regional software quality maintenance similar to the International Organization for Standardiza-

tion's (ISO) 9000 guidelines[62] for quality manufacturing processes. More than 80 countries have adopted the ISO 9000 for consistency in manufacturing processes. ISO 9000 requires that manufacturers produce explicit documentation for accepted procedures for all business activities; implement methods to prove that procedures are followed correctly and perform their intended functions; conduct audits of process quality; and implement improvements or corrections when problems are detected. The SOCs would monitor procedures by which an institution goes through operational needs assessment; specification of desired system functions; selection of vendors' products (or local product design and development); testing of products in a realistic environment before going "live"; adequate training of prospective users; installation and follow-up during and after installation of software systems; monitoring of users' competencies and complaints; and the adequate provision of a "help desk" tied to documentation procedures and methods for making software improvements. SOCs could help ensure that institutions build clinical enterprises to-

Table 2B ◼

Proposed Classes of Clinical Software Exemptions and Regulation by Category of Software

Type of Software	Description
Class B	Software Exempt from FDA regulation; local SOC monitoring required. (Please refer to definitions of risk categories and regulatory classes in Table 1.)
All Category 1	All low-risk, patient-specific, low-impact software giving adequate control to licensed practitioner (easily overridden).
Some Category 2	Intermediate-risk, high-impact patient-specific software giving adequate control to licensed practitioner (easily overridden), including locally developed or "shareware" non-commercial software systems; local SOC monitoring recommended for such software. EXCEPT: Category 2 systems commercially distributed that are not modified in any way locally and that do not serve as part of an integrated local system.
Some Category 3	Locally developed, non-commercial, patient-specific, high-impact systems with minimal ability of practitioner to override. It is mandatory, on an ethical basis, that such systems have careful local review and institutional oversight through both IRBs and SOCs. Such systems should adhere to product labeling standards and be registered for simple identification purposes with FDA, even though non-commercial. EXCEPT: Category 3 systems distributed commercially.

Table 2C ■

Proposed Classes of Clinical Software Exemptions and Regulation by Category of Software

Type of Software	Description
Class C	Software subject to simplified, expedited initial FDA approval through verification that product labeling is accurate and adheres to standards; mandatory listing of products with FDA for post-marketing surveillance; application of usual FDA 510(k) or PMA processes to any products generating concerns during post-marketing surveillance; local SOC monitoring mandatory. (Please refer to definitions of risk categories and regulatory classes in Table 1.)
Some Category 2	Intermediate-risk, high-impact, patient-specific software giving adequate control to licensed practitioner (easily overridden), commercially distributed and not modified in any way locally.

ward a reference architecture with a modular design so that components can be replaced as they are outdated.

SOCs would work with system administrators, users, and vendors to make sure there is ongoing monitoring to detect adverse events, address them, and to insure that the overall system performs as designed; and, that adequate attention is paid by vendors to make sure that vendor-product related problems detected are corrected in a timely manner (appropriate for the clinical risk posed by the problem). It would also be important to develop ethical guidelines that would specify behavior for employees and SOC committee members who might have special relationships with vendors or have software-related companies of their own.

Explanation of Recommendation 3: A Focused FDA Strategy for Exemption and Regulation of Clinical Software Systems

The consortium recommends local oversight of clinical software systems through SOCs (as described above) whenever possible, and adoption by health care information system developers and vendors of a code of good business practices (see Explanation of Recommendation 4, below). Governmental regulators have a legislative obligation to play a meaningful role in assuring patient safety. To maximize benefit of FDA efforts, we believe that the agency should focus on those commercial stand-alone systems presenting the highest degree of clinical risk (as defined in Tables 1A and 2A to 2D). The FDA should move to formalize the spirit of the 1989 FDA draft policy[54] in a clearly

worded new policy. The FDA should now define explicitly the categories of clinical software systems that will be exempt from its regulation. Recently, the Center for Healthcare Information Management (CHIM) has prepared an algorithm, expressed in the form of a flow sheet, suggesting how the FDA might go about classifying stand-alone clinical software systems for regulatory purposes (see Appendix). This document has not been reviewed for endorsement by consortium members. However, the document is consistent, for the most part, with the portion of consortium recommendations related to the FDA.

Other than exemption, the two actions now available to FDA for medical software devices—the 510(k) process and the PMA process—are inappropriately cumbersome for all but the highest risk category of clinical software systems. However, the FDA might serve a less intrusive monitoring role by requiring producers of exempt clinical software systems to list them as products with the FDA for monitoring purposes, without having to undergo the 510(k) or PMA processes. By assigning a universal registration ID to each product, the FDA could develop a centralized database repository for collecting information on adverse clinical software events. Reporting of problems with individual products could come to the FDA through SOCs, or from individual users in sites without SOCs. The FDA could then collect and distribute aggregated, standardized reports of system-specific and global problems (including interactions).

Another beneficial role the FDA could play would be to develop, in conjunction with vendors, clinical sites, professional organizations, and users, new, comprehensive standards for clinical software product labeling. Labels should describe system requirements, functions, document sources of medical information, and describe limitations of use. Labeling standards for

Table 2D ■

Proposed Classes of Clinical Software Exemptions and Regulation by Category of Software

Type of Software	Description
Class D	Software subject to FDA 510(k) and PMA approval before marketing; Local SOC monitoring mandatory. (Please refer to definitions of risk categories and regulatory classes in Table 1.)
Some Category 3	High-risk, high-impact, patient-specific software giving adequate control to licensed practitioners (not easily overridden), commerically distributed and not modified significantly locally. Systems would also adhere to product labeling standards.

clinical software would be different than existing FDA standards developed primarily for hardware medical devices. The FDA could require manufacturers of both exempt and non-exempt software products to adhere to the labeling standards. As noted in Table 2C, the FDA could modify its approach to certain intermediate-risk commercial products by creating an expedited process to verify that the product's labeling conforms to FDA standards. The FDA would then assign a post-marketing surveillance ID to such products and carefully monitor for evidence of adverse effects. If a sufficient number of concerns were raised during product monitoring, the manufacturer would then be required to submit full-scale 510(k) or PMA applications to be permitted to continue marketing.

Explanation of Recommendation 4: Adoption of Guidelines by Clinical Software Producers and Distributors

The health care information system industry, through the Center for Healthcare Information Management (CHIM), is in the process of refining its code of good business practices. This code, in conjunction with ISO-9000, is expected to address use of sound software development and implementation methods appropriate to the level of clinical risk posed by a software system. It will also address the need for adequate training, for support of open industry standards for messages and communication, for protecting patient confidentiality, and for other relevant matters. Adherence to the guidelines should be strongly encouraged for all clinical software systems, and be mandatory for higher-risk systems. The FDA Current Good Manufacturing Procedures (CGMPs) for individual products may not work effectively for the complex software environments in large health care delivery facilities (see Fig. 1). The FDA currently requires medical device manufacturers to comply with ISO-9000-like regulations as part of their manufacturing process. Through SOCs, local institutions should develop guidelines for the acquisition, testing, installation, training, and monitoring of the potentially complex systems under their control, in the spirit of ISO-9000. Local SOCs should also oversee implementation and monitoring of local guidelines, and interinstitutional sharing of experiences.

Examples of guidelines for good business practices include the following: Manufacturers should disclose existing evaluations of software products (noting how they relate, if at all, to the current product) for users to review before purchasing systems. Developers should help users to estimate how often and by what mechanism system components—including databases or knowledge bases, as well as software code—need

to be upgraded or replaced. Users and/or external reviewers should determine if upgrades are of professional quality. Vendors and users should verify that upgrades are made available or distributed to all who should receive them. Vendors should help local users to ensure that only users who are well qualified (i.e., possess sufficient biomedical knowledge) and well trained (i.e., have adequate skill in using the program) will have access to a given clinical software system. In addition to standard software version control practices, developers should document sources and dates of creation/revision for biomedical knowledge embedded in software programs. Manufacturers should disclose any known risks and limitations associated with a clinical software product, and inform users of their responsibility to detect and override faulty system recommendations. "Outdated" systems should advertise to users that their components are potentially invalid—e.g., through start-up screens that force users to acknowledge that the system is outdated before allowing the users to proceed, or through prominent banners displayed at all times during system usage. If warnings are not adequate for high-risk or significantly compromised outdated components, the system might simply prevent users from using outdated functions by removing access to the functions from the system. Vendors, as well as regulators, should provide standardized forms and convenient avenues for problem reporting. Manufacturers should ensure that notification procedures are in force for higher-risk product categories to ensure users are aware of product alerts, recalls, and upgrades. Manufacturers should continue to utilize guidelines that protect patients and users through the expedited, efficient testing of new system components and upgrades. Last but not least, manufacturers should adopt and adhere to, whenever possible, national or international standards for data representation and exchange.[63]

Explanation of Recommendation 5: Collaboration to Evolve Clinical Software Monitoring and Regulation

Institutions with installed advanced health care information systems should implement SOCs and share their experiences and recommendations with others. The expanded consortium, consisting of clinical professional associations, vendor organizations, regulatory agencies, and user communities, should evolve the guidelines contained in recommendations 1 through 4 as they gain increasing experience with approaches to monitoring and regulating clinical software systems. Focus groups, the peer-reviewed literature, regional and national conferences, Internet-

based information resources, and other means should be used to disseminate the information.

Summary

Clinical software systems are ubiquitous. A growing literature documents the benefits of such systems for improved health care delivery. While no reports suggest that many patients are being harmed by stand-alone clinical software systems, concerns for patient safety must be addressed. The consortium recommends local oversight of clinical software systems through Software Oversight Committees (SOCs), and adoption by health care information system vendors of a code of good business practices. Budgetary and other constraints limit the type and number of systems that the FDA can regulate effectively. Most clinical software systems should be exempted from FDA regulation. FDA regulation should focus on patient-specific commercial software systems that pose high clinical risk (e.g., directly control life support systems or directly administer potentially dangerous therapies) that are not modified locally (i.e., are not under local programming control) and which offer little or no opportunity for practitioner intervention. For such "closed loop" systems, based on the degree of risk posed, we recommend the traditional FDA 510(k) notification process and full-scale pre-market approval. During pre-market trials for such narrowly defined, high-risk, closed loop systems, it must be demonstrated that the systems cause no harm, or, alternatively, that the automated systems improve upon imperfect baseline (manual) systems at a tolerable (non-zero) level of risk and at an affordable cost.

We have provided recommendations on how to develop and realize processes for responsible monitoring and regulation of clinical software systems. Our goal is to encourage a coordinated effort to safeguard patients, users, and institutions as clinical systems are implemented to improve clinical care processes.
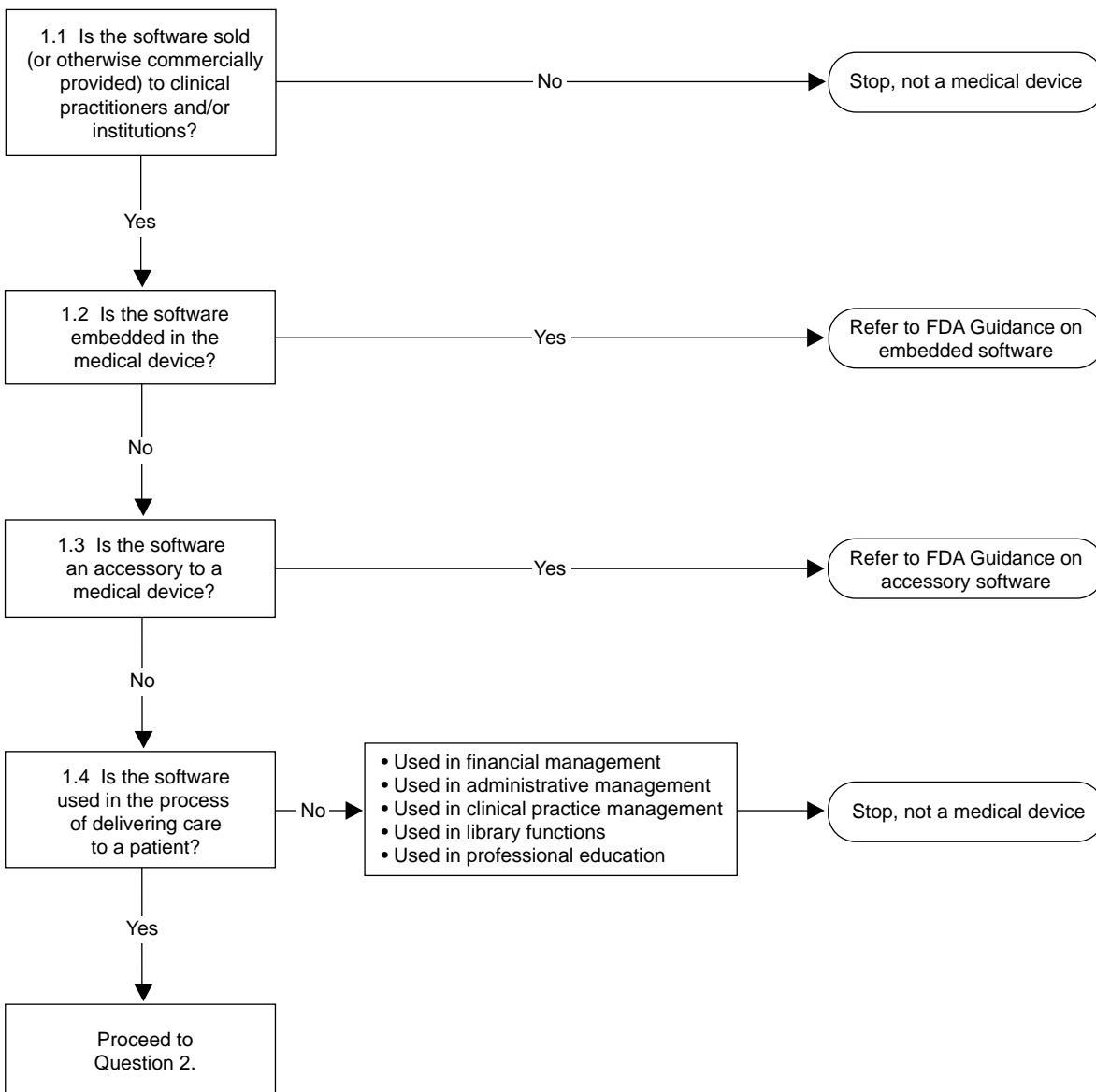
References ■

1. Federal Register. July 15, 1996. 61:36886–7.
2. Food and Drug Administration Center for Devices and Radiological Health. Announcements and minutes of meetings on future regulation of stand-alone clinical software systems. 1996–1997. FDA Web site: http://www.fda.gov/cdrh
3. AMIA News. J Am Med Inform Assoc. 1994;1:91–2.
4. Institute of Medicine. Dick RS, Steen EB (eds). The computer-based patient record: an essential technology for health care. Washington DC: National Academy Press. 1991.
5. Ball MJ, Collen MF (eds). Aspects of the Computer-based Patient Record: Computers in Health Care Series. New York: Springer-Verlag, 1992.
6. Kuperman GJ, Gardner RM, Pryor TA. HELP: A Dynamic Hospital Information System. New York: Springer-Verlag, 1991.
7. McDonald CJ, Tierney WM, Overhage JM, Martin DK, Wilson GA. The Regenstrief Medical Record System: 20 years of experience in hospitals, clinics, and neighborhood health centers. MD Comput. 1992;9:206–17.
8. Barnett GO. The application of computer-based medical record systems in ambulatory care. N Engl J Med. 1984;310:1643–50.
9. McDonald CJ, Tierney WM. Computer-stored medical records: their future role in medical practice. JAMA. 1988;259:3433–40.
10. Garrett LE Jr, Hammond WE, Stead WW. The effects of computerized medical records on provider efficiency and quality of care. Meth Inform Med. 1986;25:151–7.
11. Rector AL, Glowinski AJ, Nowlan WA, Rossi-Mori A. Medical-concept models and medical records: an approach based on GALEN and PEN&PAD. J Am Med Inform Assoc. 1995;2:19–35.
12. Yount RJ, Vries JK, Councill CD. The Medical Archival System: an Information Retrieval System based on Distributed Parallel Processing. Information Processing & Management. 1991;27:379–89.
13. Vries JK, Yount RJ, Singh J: Total integration of health center information through distributed parallel processing. HIMSS Proceedings. 1994;4:241–52.
14. Warner HR, Toronto AF, Veasey LG, Stephenson RA. Mathematical approach to medical diagnosis. JAMA. 1961;177:75–81.
15. Gorry GA, Barnett GO: Experience with a model of sequential diagnosis. Computers & Biomedical Research. 1968;1:490–507.
16. Bleich HL. Computer evaluation of acid-base disorders. J Clin Invest. 1969;48:1689–96.
17. Horrocks JC, McCann AP, Staniland JR, Leaper DJ, de Dombal FT: Computer-aided diagnosis: description of an adaptable system, and operational experience with 2,034 cases. Br Med J. 1972;2:5–9.
18. Pauker SG, Gorry GA, Kassirer JP, Schwartz WB: Toward the simulation of clinical cognition: taking a present illness by computer. Am J Med. 1976;60:981–96.
19. Shortliffe EH. Computer-Based Medical Consultations: MYCIN Artificial Intelligence Series. New York: Elsevier Computer Science Library, 1976.
20. Yu VL, Fagan LM, Wraith SM, et al: Antimicrobial selection by computer: a blinded evaluation by infectious disease experts. JAMA. 1979;242:1279–82.
21. Blois MS. Judgement and computers. N Engl J Med. 1980;303:192–7.
22. Miller RA, Pople HE Jr, Myers JD: Internist-1: an experimental computer-based diagnostic consultant for general internal medicine. N Engl J Med. 1982;307:468–76.
23. Barnett GO, Cimino JJ, Hupp JA, Hoffer EP: DXplain: an evolving diagnostic decision-support system. JAMA. 1987;258:67–74.

24. Warner HR, Haug P, Bouhaddou O, et al. ILIAD as an expert consultant to teach differential diagnosis. Proc Twelfth Ann Symp Comput Appl Med Care. New York: IEEE Computer Society Press, 1987;371–6.

25. Bankowitz RA, McNeil MA, Challinor SM, Parker RC, Kapoor WN, Miller RA: A computer-assisted medical diagnostic consultation service. Implementation and prospective evaluation of a prototype. Ann Intern Med. 1989;110:824–32.

26. Miller RA. Medical diagnostic decision support systems—past, present, and future. J Am Med Inform Assoc., 1994;1:8–27.

27. McDonald CJ. Protocol-based computer reminders, the quality of care and the non-perfectability of man. N Engl J Medicine. 1976;295:1351–5.

28. McDonald CJ, Wilson GA, McCabe GP Jr. Physician response to computer reminders. JAMA. 1980;244:1579–81.

29. Tierney WM, Hui SL, McDonald CJ. Delayed feedback of physician performance versus immediate reminders to perform preventive care: effects on physician compliance. Medical Care. 1986;24:659–66.

30. Tierney WM, McDonald CJ, Martin DK, Rogers MP. Computerized display of past test results: effect on outpatient testing. Ann Intern Med. 1987;107:569–74.

31. Tierney WM, McDonald CJ, Hui SL, Martin DK. Computer predictions of abnormal test results: effects on outpatient testing. JAMA. 1988;259:1194–8.

32. McDonald CJ. Computers. JAMA. 1989;261:2834–6.

33. Tierney WM, Miller ME, McDonald CJ. The effect on test ordering of informing physicians of the charges for outpatient diagnostic tests. N Engl J Med. 1990;322:1499–504.

34. McDonald CJ, Overhage JM. Guidelines you can follow and can trust: an ideal and an example. JAMA. 1994;271:872–3.

35. Evans RS, Larsen RA, Burke JP, et al. Computer surveillance of hospital-acquired infections and antibiotic use. JAMA. 1986;256:1007–11.

36. Pestotnik SL, Evans RS, Burke JP, Gardner RM, Classen DC. Therapeutic antibiotic monitoring: surveillance using a computerized expert system. Am J Med. 1990;88:43–8.

37. Gardner RM, Golubjatnikov OK, Laub RM, Jacobson JT, Evans RS. Computer-critiqued blood ordering using the HELP system. Computers & Biomedical Research. 1990;23:514–28.

38. Classen DC, Evans RS, Pestotnik SL, Horn SD, Menlove RL, Burke JP. The timing of prophylactic administration of antibiotics and the risk of surgical-wound infection. N Engl J Med. 1992;326:281–6.

39. Hickam DH, Shortliffe EH, Bischoff MB, Scott AC, Jacobs CD. The treatment advice of a computer-based cancer chemotherapy protocol advisor. Ann Intern Med. 1985;103:928–36.

40. Musen MA, Carlson RW, Fagan LM, Deresinski SC, Shortliffe EH. T-HELPER: automated support for community-based clinical research. Proc Annu Symp Comput Appl Med Care. 1992;719–23.

41. Institute of Medicine. Telemedicine: A Guide to Assessing Telecommunications in Health Care. Washington, DC. National Academy Press, 1996.

42. Willems JL, Abreu-Lima C, Arnaud P, et al. The diagnostic performance of computer programs for the interpretation of electrocardiograms. N Engl J Med. 1991;325:1767–73.

43. Becker SH, Arenson RL. Costs and benefits of picture archiving and communication systems. J Am Med Inform Assoc. 1994;1:361–71.

44. McDonald CJ. The barriers to electronic medical record systems and how to overcome them. JAMIA. 1997;4:222–32.

45. Slack W (ed). Medical hardware and software buyer's guide. MD Comput. 1996;13:485–576.

46. Friedman CP, Wyatt JC. Evaluation methods in medical informatics. New York: Springer-Verlag, 1997.

47. Stead WW, Haynes RB, Fuller SL, et al. Designing medical informatics research and library-resource projects to increase what is learned. J Am Med Inform Assoc. 1994;1:28–34.

48. Tierney WM, Overhage JM, McDonald CM. A plea for controlled trials in medical informatics. J Am Med Inform Assoc. 1994;1:353–4.

49. Schoolman HM. Obligations of the expert system builder: meeting the needs of the user. MD Comput. 1991;8:316–21.

50. East TD, Morris AH, Wallace CJ, et al. A strategy for development of computerized critical care decision support systems. Intl J Clin Monit Comput. 1992;8:263–9.

51. Miller RA. Why the standard view is standard: people, not machines, understand patients' problems. J Med Philos. 1990;15:581–91.

52. Miller RA, Schaffner KF, Meisel A. Ethical and legal issues related to the use of computer programs in clinical medicine. Ann Intern Med. 1985;102:529–36.

53. Public Law 94-295. Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act (passed on May 28, 1976).

54. Young FE. Validation of medical software: present policy of the Food and Drug Administration. Ann Intern Med. 1987;106:628–29.

55. FDA Center for Biologics Evaluation and Research, Office of Blood Research and Review, Office of Compliance, Office of Regulatory Affairs. Draft Guideline for the Validation of Blood Establishment of Computer Systems. Issued September 20, 1994. Available from FDA WWW Site: http://www.fda.gov

56. FDA Center for Biologics Evaluation and Research, Office of Blood Research and Review. Draft Reviewer Guidance for a Pre-Market Notification Submission for Blood Establishment Computer Software. Issued April 12, 1996. Available from FDA WWW Site: http://www.fda.gov

57. FDA Center for Devices and Radiological Health. Guidance for the Content and Review of 510(K) Notifications for Picture Archiving and Communications Systems (PACS) and Related Devices, Issued August 1, 1993. Available from FDA WWW Site: http://www.fda.gov//cdrh/ode/odeot416.html

58. FDA Center for Devices and Radiological Health. Telemedicine Related Activities. Issued July 11, 1996. Available from FDA WWW Site: http://www.fda.gov//cdrh/telemed.html

59. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Ethical principles and guidelines for the protection of human subjects of research (The Belmont Report). Federal Register, Document 79-12065, April 17, 1979.

60. Protection of Human Subjects. Code of Federal Regulations, Title 45, Part 46, June 18, 1991.

61. FDA. FDA information sheets for IRBs and clinical investigators. Issued October 1, 1995. Available from FDA WWW Site: http://www.fda.gov

62. Organization for International Standards. ISO 9000 News Service, 1996–97. Documentation available from: http://www.iso.ch

63. AMIA Board of Directors. Standards for medical identifiers, codes, and messages needed to create an efficient computer-stored record. J Am Med Inform Assoc. 1994;1:1–7.

Appendix Flow diagram prepared by Center for Healthcare Information Management (CHIM) Suggesting Possible Decision Algorithm for FDA to Use in its Regulation of Stand-alone Clinical Software Systems as Medical Devices.

Question 1. Is the "stand-alone" software a medical device?

1.1 Is the software sold (or otherwise commercially provided) to clinical practitioners and/or institutions?	——No——▶ Stop, not a medical device
↓ Yes	
1.2 Is the software embedded in the medical device?	——Yes——▶ Refer to FDA Guidance on embedded software
↓ No	
1.3 Is the software an accessory to a medical device?	——Yes——▶ Refer to FDA Guidance on accessory software
↓ No	
1.4 Is the software used in the process of delivering care to a patient?	——No——▶ • Used in financial management • Used in administrative management • Used in clinical practice management • Used in library functions • Used in professional education ——▶ Stop, not a medical device
↓ Yes	
Proceed to Question 2.	

Question 2. What are the risks or hazards associated with and the level of concern for the "stand-alone software"?

2.5 Checklist to establish suitability for exemption from active regulation

Software provides or replaces existing software applications with well understood functions and no history of adverse events. — Yes

Software automates well-understood manual/paper based processes. — Yes

Software simply manages data from clinicians. — Yes

Software allows intended/competent user intervention. — Yes

Software allows competent user organization to evaluate and test. — Yes

Software assures back-end integrity. — Yes

System failure does not cause software to add risk to patient. — Yes

Software automates difficult manual/paper based functions. — Yes

Software monitors events and alerts but takes no action.

Yes   Yes

2.6 Is software characterized by one or more indicators? — No → Re-evaluate.

Yes

2.7 Will complete, accurate labeling provide user with adequate information to use safely? — No → Re-examine.

Yes

2.8 Software is exempt from active regulation.