Software Quality Regulation Under the Safe Medical •Devices Act of 1990: Hospitals Are Now the Canaries in the Software Mine

Vincent M. Brannigan J.D.
University of Maryland,
College Park Md. 20742
301-657-1410 vb15@umail.umd.edu

Abstract

The 1990 Medical Device Amendments to the Food and Drug Act have caused a significant change in the regulation of medical software. The 1990 Act replaces the prior emphasis on premarket approvals with an emphasis on postmarket surveillance. Hospitals and other institutional users are now required to report to the FDA product defects that cause injuries or death. They are also required to report product defects to the manufacturer. The Act provides for rapid suspensions of device approval, recalls of defective products and civil penalties for violators. The combination of these factors may lead to enhanced FDA supervision of the purchase and use of medical software, and particularly an emphasis on finding unregistered producers. In addition, the new Act will have a direct effect on the regulation of software, because it is much better suited to addressing the problem of software quality than the 1976 Act.

Introduction

The SAFE MEDICAL DEVICES ACT OF 1990 is a comprehensive change in the medical device requirements of the Food and Drug Act. The changes affect both medical software developers and users. Under the new law Congress has accepted the FDA's development of simple premarket approval for getting products on the market, but has developed a regulatory system which requires device related injuries to be promptly reported to the FDA. Hospitals and other institutional providers of health care will need to put in place new reporting systems. Like the canary in a mine, hospitals will be expected to sound the early warnings of dangerous conditions, so the FDA can take remedial action.

Is Software a Medical Device ?

The 1990 Act has made no change in the fundamental definition of medical devices. The Medical Device Amendment of 1976 defines devices:

(h) "device"...means an instrument, 2) intended for use in the diagnosis of disease or other conditions, or in the cure...or prevention of disease...21 USCS @ 321 (1990).

There is a commonly held belief promoted by some members of the medical software industry that software that provides for competent human intervention before a patient is injured is not a medical device. This is simply not the law, for software or any other device. A thermometer provides information to the caregiver. The caregiver then has an opportunity for competent human intervention. However **the thermometer is still a device**, since it is an "instrument which is....intended for use in the diagnosis of disease". Software which is used in a medical device is clearly a device. Software that is used to connect devices together is a medical device under most circumstances. Insofar as a software system is sold for the purpose of channeling information to or from medical devices, in the author's opinion such software is itself a medical device.

The furthest reach of FDA jurisdiction may be open to some question, especially in regards to certain stand alone expert systems. [1,7,8,9,10,11] However, as a matter of law, the FDA asserted a wide jurisdiction over medical software, and Congress enacted new legislation without challenging that assertion. This could easily be construed as Congressional acquiescence in the assertion of jurisdiction.

Because of the substantial penalties for failure to register as a medical device manufacturer, no manufacturer who sells software for any medical purpose can assume that they are not required to file as a device manufacturer. If in doubt, the FDA should be consulted. At a minimum, competent counsel with expertise in FDA regulated software should be

0195-4210/91/$5.00 © 1992 AMIA, Inc.

consulted to determine the status of any given software product, prior to marketing or purchasing the software.[5] However, this type of good faith reliance on counsel's advice would at most Act to reduce penalties under the Act. It would not affect the regulated nature of the product. The FDA is aware of and responding to the failure of software vendors to register under the Act. Failure to register can lead to civil and criminal penalties. Further, the structure of the new Act and the new approach to enforcement may lead to targeting of unregistered manufacturers. In particular, the 1990 Act gives the FDA many more tools to penalize unregistered manufacturers.

Responsibilities of Hospitals and Other Institutions

Hospitals and other institutions (but not individual physicians) now have specific new reporting obligations under the Food and Drug Act. Hospitals also face substantial liability for defective devices. [3] Many vendor's contracts limit the hospital's remedies against the vendor. It is not clear who would bear the consequences of a software failure or a regulatory recall. Especially given the simplified methods of approval in the 1990 Act, hospitals should insist that vendors warrant that software is in compliance with the Food and Drug Act.[5] An appropriate clause might be:

Vendor warrants that the software products licensed hereunder are in compliance with the Medical Device Amendments of the Food and Drug Act, and that Vendor will comply at all times with such Act.

The FDA Device establishment number for the manufacturer of this device is _____________. The 510 (k) or PMA number for this device is ______________.

This express warranty may not be disclaimed, nor may remedies be limited. Purchaser may revoke the acceptance of any software not in compliance with the Food and Drug act. Vendor will promptly notify purchaser of any report made to the Food and Drug administration by any party concerning any defect of any kind in the licensed software.

The failure to confirm that the manufacturer of software has obtained FDA registration of the device might subject the institution to punitive damages to an injured patient.

Regulation of Medical Devices

Under the 1976 Act the device manufacturer must register with the FDA and file the required annual reports. The manufacturer must file a premarket notification prior to putting the device on the market. The manufacturer must follow the "good manufacturing practices" required by the appropriate regulations. These requirements have not changed. What has changed in the 1990 Act is the regulatory philosophy. Under the 1976 Act, devices were put into three classes, according to risk, with increasing stringency of regulations. However, the FDA found the statute unworkable. To cope with the load, the FDA adapted a minor section of the Act, the 510 (k) procedure, to approve 95% of all medical devices. This section of the Act had been designed as a transitional section, and operated by "grandfathering" devices which were "substantially equivalent" to pre 1976 devices. The FDA adapted the 510 (k) by demanding substantially more information than was needed to determine substantial equivalence. The industry cooperated because the alternative, premarket approval, was much worse. The 1990 Act changed the Food and Drug Act treatment of section 510(k) to conform it to the FDA practice. The statute explicitly allows the FDA 510 (k) approval, but with strengthened reporting and enforcement mechanisms. Despite Congress's ratification of the FDA actions, it appears clear that Congress intends the FDA to take a new approach to device regulation. The 1990 Act accepts that it will be somewhat easier for products to go on the market than if the FDA had actually enforced the 1976 act, but there will be more stringent post market surveillance, with aggressive data gathering and enforcement. Under the new statute hospitals and other institutions are the key detection system for defective products. The 1990 Act implements this postmarket approach by a combination of easier market entry, greater surveillance and rapid regulatory reaction.

Device Marketing

Congress codified the 510 (k) procedure but increased the power of the FDA to demand detailed information from the manufacturer. Congress eliminated the requirement of substantial equivalence to pre 1976 devices, only requiring equivalence to pre 1990 devices. However, the filing requirements clearly put a burden on the manufacturer to supply all relevant data to the FDA, not merely that which shows substantial equivalence. Congress also introduced the new concept of "special controls". Special controls are oriented towards postmarket activities and include both device controls and reporting requirements. (Section 513(a)(1)(B)) The development of special controls should allow FDA to put products on the market more quickly, since they will be utilized under more controlled conditions.

Data Collection

Hospitals and other institutional users (device user facilities), but not doctors, now have to report deaths related to medical devices **directly to the FDA**. Section 519 (b)(1)(A) Hospitals and other institutional users now have to report injuries to the manufacturers, and then twice a year report such injuries to the FDA. These reports cannot be introduced in malpractice actions, but the failure to make such a report might itself invite liability to other patients injured by the same device.

Manufacturers have to report to the FDA all alterations or repairs to devices in the field that are related to product safety. **This would include any correction of software errors that affect patient safety.** Section 519 (21 U.S.C. 360i), (f)(1) For life critical devices, such as intensive care unit monitors, manufacturers must put into place an FDA approved surveillance system for product defects. (Sec. 521)

Enforcement

Under the 1990 Act the FDA can now temporarily suspend a device approval for a device (Section 515(e)(3)), order a halt to distribution and use (Section 518 (e)(1)) and impose a civil penalty of $ 15,000 per violation and $1,000,000 per proceeding. Agencies prefer civil penalties because they are handled administratively within the agency, the burden of proof is preponderance of the evidence, rather than beyond a reasonable doubt, and the agency can set policies on how large a penalty to collect.

In the past, the FDA focussed on approving submitted devices and inspecting registered medical device manufacturers, and had limited tools for discovering unregistered vendors. Now the FDA has the tools to find unregistered manufacturers, and given the regulatory structure, can be expected to make targeting such manufacturers a high priority. Computer matching of device reports and registered manufacturers will pinpoint both vendors who are not registered and users who are not making the required reports.

Software Quality

At the same time that the FDA will be dealing with the problem of unregistered software manufacturers, they will deal with the persistent problems of software quality. The causes of software quality problems are complex, but in general they have to do with the nature of software development. Real time, programmable interactive digital equipment was unknown anywhere 25 years ago. The use of computers originated in financial and inventory accounting and scientific calculations. the work was batch processed and normally not time critical. These fairly simple tasks set a relatively low standard for quality control and system reliability, compared to typical medical devices. The work pattern that developed was simple functional testing before the software release. Software developers, pressed for time by their managers, often assumed that the bugs would be discovered by the customers and reported. They would be addressed in the next "software update". The customer could then be charged for "program maintenance".

Compared to traditional programs, medical information systems are complex, sophisticated and powerful. In addition, the possibility for disastrous software failure has also increased, because the ability to manage the hazard or regulate the risk does not necessarily increase with the functional capability. Medical computer software is an area where neither the vendors nor the regulators have good tools for ensuring quality. The software industry has neither good ways of breaking down software jobs into reliable components, nor simple means of defining and testing a finished product. System documentation is often done after the system is written, if someone thinks of it, if someone will pay for it, if the software developer is still interested in it, and if someone can still figure out what was done.

Companies often go into a new technology with inadequate technological supervision. Companies have no formal analysis of technological and regulatory risks. There is usually a misplaced reliance on the ability of the government to regulate, and an attitude of doing the bare minimum insisted on by the regulators. "Show me the regulation" is a typical response by many corporate executives, who are unaware that their present actions will be judged in the future by the regulatory authorities and the courts, not based on the current regulations, but on the future regulatory and liability climate. [9]

Regulatory agencies have their own problems. They try to fit new technologies into existing statutes and bureaucracies. The fit is often poor, but the institutional factors overwhelm the need to actually understand the new technology. Typically, not enough resources are allocated to do the job. [4]

Software has distinct characteristics which make both quality management and regulation difficult. The first is the nature of production. Unlike anything else of equivalent sophistication, software is still fundamentally an individual creation. A surprising number of software products on the market are essentially one person's work. It is difficult and very time consuming even for another software expert to analyze and critique software, without the cooperation of the software developer. In addition, planning and subdividing software development is very difficult. It is widely accepted that it is impossible to test all paths, and therefore impossible to remove all software bugs from code. Bugs can wreak havoc years after the software is released for use.

Software developers have flourished in an environment in which specification of the design was not rigorous, and quality control over the output was not enforced. This system meant that software regulation under the 510 (k) process was essentially ineffective. There simply was no way to look at the type of software documentation submitted and determine that it was a good design. However, under the new regulatory environment, the concentration of the regulatory system will be on "bugs", with the FDA alerted every time a software defect appears. Hospitals will be under a strict legal obligation to report problems which could affect patient safety. **Vendors will have to report any patient safety related software modifications.** The widespread publicity accorded to recalls should force vendors to develop new and more effective quality control efforts.

Analysis

The combination of easier approvals, stepped up data collection and increased remedial actions and penalties creates a totally new environment for FDA regulation of software. In effect, the Congress recognized that trying to control the safety of devices before they are marketed is largely futile, but reacting quickly to defective devices after they are marketed is absolutely critical. While Congress probably did not have software in mind when it wrote the statute, the Act is well adapted to the special problem of regulating software products. Post-market regulation is especially appropriate when:

1) Small producers are competing with large firms and there is a political desire to increase market entry. Congress has noted the small size of medical device manufactures and is sensitive to entry barriers such as premarket approval.

2) Enforcement resources are limited. The FDA has received little or no increased budget to handle the flood of medical devices. Concentrating on injuries limits the problem of effort wasted on non hazardous devices.

3) Techniques for determining relative hazards are not well developed. In many cases, it is only possible to rule out the most obvious hazards in the premarket regulation. Software poses special problems in this area. The industry has not developed good tools for validation and verification of software, and risk analysis for the use of software is in its infancy.

4) Injuries are relatively rare events. If injuries related to the devices are common, premarket regulation is the preferred approach, even at the cost of slowing introduction to the marketplace.

5) The product related to the injury is subject to continuous regulatory control. The new statute requires a system of tracking life critical devices to allow for speedy correction and recalls.

6) There is a practical system for implementing postmarket surveillance. Most of the software are used in relatively tightly controlled settings by licensed practitioners.

7) It is relatively easy to connect the injury to the injury causing activity. If injuries cannot be connected to the injury causing behavior, no regulatory system may function adequately. however, postmarket surveillance can allow epidemiological analysis of the consequences of the use of devices. Such programs have been successful in the reduction of injuries due to radiation.

Under the statute, the FDA will receive reports of deaths and injuries directly from the hospitals using a device. If a simple computer matching is performed, the FDA can very easily determine whether a device manufacturer is registered and whether the product has been approved. By monitoring vendor's activities in repairing software, the FDA will build experience in which vendors and industries have a focus on quality and which ones do not. Discovering unregistered manufacturers will become easier, and the focus on injuries and deaths will sharpen the regulatory response. Given the FDA's history, attempts to avoid FDA compliance by failing to register can be expected to result in the stiffest penalties. The FDA will also focus on whether the firm has maintained proper records of software development and testing. They will be particularly alert for a pattern of releasing inadequate software and trying to fix it in the field.

Software systems can expect to be a major FDA target, for several reasons. Cost control pressures are forcing hospitals to use computer systems to substitute for human resources.[6] Automated medical devices with computer controlled inputs and outputs are easy to connect to computer networks but failure of such systems may lead to rapid patient injury. All of these factors will lead to increased FDA scrutiny.

This is a major change in the environment for software manufacturers and users. Previously the FDA had no easy method of finding software that interacts with medical devices, and had no simple method of enforcing compliance. Now if a hospital report contains the name of a software manufacturer who has not registered, the FDA can stop shipment, and assess civil penalties of $15,000 per system. If the device is shown to be related to the injury, the FDA can order a recall of the system. The consequences for both hospitals and manufacturers of unregistered systems can be devastating. Hospitals that have not insisted that the vendors be in compliance with the Food and Drug Act will be in a very weak position to protest the disruption of operations. Even for registered systems, the tightened FDA regulation of changes in the system can be expected to lead to major emphasis on improved quality control.

Conclusion

Up to this time many software producers have not complied with the Food and Drug Act, and the FDA had the authority but not the tools to compel compliance. Hospitals and other users have been essentially indifferent to whether software was FDA registered. The 1990 Act gives the FDA the data collection and enforcement tools to track down unregistered software manufacturers. It is reasonable to expect that unregistered device manufacturers and users will be a high priority target. An enhanced FDA emphasis on software quality may improve the overall software environment.

References

1.Brannigan V. **Legal Issues in Medical Computing** In Encyclopedia of Medical Devices and Instrumentation John Wiley and Sons, New York 1989 1742-1749

2.Brannigan V. and Mola E. **Liability for the use of Computers in Obstetrics and Gynecology** in Dalton, K and Chard T. Computers in Obstetrics and Gynecology, Elsevier, Amsterdam 1990 287-298

3.Brannigan, V. and R. Dayhoff, **Liability for Personal Injuries Caused by Defective Medical Computer Programs**, American Journal of Law and Medicine, 2, Summer, 1981, pp. 123-144.

4.Brannigan, V., **Compensation or Regulation, the Problem of Medical Computer Software**, Journal of Consumer Policy, 1983,Vol. 6:475-481.

5.Brannigan, V., **Acceptance Testing: The Critical Issue in Software Acquisition**, IEEE Transactions on Biomedical Engineering, (1985) Vol. 32:295-299.

6.Brannigan, V., and Dayhoff, R., **Medical Informatics: The Revolution in Law, Technology and Medicine**, Journal of Legal Medicine, March 1986, vol 7:1-53.11.

7.Brannigan, V., **The Regulation of Medical Software as a Device Under The Food, Drug and Cosmetic Act** Jurimetrics Journal of Law, Science and Technology, Summer 87, Vol.27,370-382.

8.Brannigan, V., **The Regulation of Medical Computer Software as a Device Under The Food, Drug and Cosmetic Act**, Proceedings of the 10th Symposium on Computer Applications in Medical Care, IEEE, 1986:347-354.

9.Health Industry Manufacturers Association **Proceedings of the HIMA conference on FDA Regulation of Medical Software, March 1988**

10.Hyman W., Brannigan V, McDermott J, Willingmyre G, and Estrin N. **Regulatory and Other Public Policy Issues** IEEE Engineering in Medicine and Biology Sept 1989 pp.33-40

11.**Information Technologies in the Health Care System**, Hearings before the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology, April 21, 1986