THE NEXT WAVE: FEDERAL REGULATORY, INTELLECTUAL PROPERTY, AND TORT LIABILITY CONSIDERATIONS FOR MEDICAL DEVICE SOFTWARE

PAUL A. MATHEW

ABSTRACT

Counsel for the medical software technologist faces an unusually complex, ongoing, high-stakes challenge. Counsel operates in a special field of commercial, legal and regulatory forces: (1) intellectual property laws which govern the expression and protection of commercial rights derived from advances in medical science and technology; (2) existing and proposed contracts/warranty laws that govern technological commercial relationships; (3) negligence, professional liability, and product liability laws that govern the marketing of medical technologies; and, (4) a new body of regulation derived from the power of the federal government to indirectly provide for the safety, effectiveness, privacy, and security of medical technologies offered to the American public. Against that backdrop, the author provides an illustration of the commercialization of a new medical software technology and suggests a general approach to resolving the primary issues facing the medical software technologist.

Cite as 2 J. MARSHALL REV. INTELL. PROP. L. 259

THE NEXT WAVE: FEDERAL REGULATORY, INTELLECTUAL PROPERTY, AND TORT LIABILITY CONSIDERATIONS FOR MEDICAL DEVICE SOFTWARE

PAUL A. MATHEW*

"We are developing molecular imaging technology, which we will use to image molecules within the body, within the cell."[1] *Elias Zerhouni*

"A dirty little secret about 802.11b is that it can cover more than 20 kilometers with suitably directional antennas. Imagine reaching places that do not have sufficient commercial value to justify classic infrastructure. In these cases, the viral nature of unlicensed telecommunications becomes a major force of human development, transforming everything from education to entertainment, hospitals to hiring halls."[2] *Nicholas Negroponte*

"No one really knows how to run a secure enterprise network system. The systems are fantastically complex, beyond human comprehension. In ten years machines will be 1000 times more complex and 1000 times more powerful. Privacy issues will loom more and more. Guidance will come from law, social pressure, and ethics."[3] *Dan Farmer*

---

* Paul A. Mathew, LL.M., Intellectual Property and Technology Law, University of Washington School of Law, and Technology Entrepreneur Certificate, University of Washington School of Business, 2002. Mr. Mathew serves as WRF Capital/Gates Technology Entrepreneurship Fellow for the Center for Technology & Entrepreneurship at the University of Washington School of Business. He is a licensed California attorney. He holds Bachelor of Science, Master of Business Administration, and Juris Doctor degrees as well as certifications in Technology Company Management and Intellectual Property Management. Mr. Mathew dedicates this article to his children Jane E Mathew and Jim Mathew. He extends his special thanks to Robert Gomulkiewicz, Esq., Director, "Intellectual Property and Policy Law Program," University of Washington, Seattle, Washington, and Andrew Klein, Professor of Law, Indiana University School of Law - Indianapolis, for their thoughtful suggestions and comments. He also wishes to thank Jean Cooley for her helpful editing assistance.

[1] Elias Zerhouni, Remarks Made During a National Public Radio "Science Friday" Broadcast (September 20, 2002) *available at* http://sciencefriday.com/pages/2002/Sep/hour1_092002.html.

[2] Nicholas Negroponte, *Being Wireless: Why Wi-Fi Lily Pads and Frogs Will Transform the Future of Telecom*, WIRED 118-19 (Oct. 2002); *see also* Nancy Gohring, *Tech 2002: Wi-Fi Blooms, Wi-Fi's Breakout Year*, SEATTLE TIMES, Dec. 9, 2002, *available at* 2002 WL 3925102. Wi-Fi, also known as WLAN or 801.11 technology, enables laptop computer users to wirelessly access the Internet within the radius of an antenna hooked to a wireline Internet connection. *Id.*

[3] Dan Farmer, Remarks Made Before the Internet Law & Policy Forum, "*Security v. Privacy*," (Sept. 18-19, 2002).

INTRODUCTION

Over the past fifty years, the United States has mobilized its national technology base, its communications structures, and its centralized regulatory and purchasing power to develop strategically important, safe, effective, and highly reliable information technology systems. For example, the United States Nuclear Regulatory Agency regulates the software used to operate American nuclear power plants.[4] The United States Department of Defense operates the world's most sophisticated and secure digital networks.[5] The effort to advance the strategic interests of the United States has led to the creation of standardized information technology practices and techniques that are being adapted for use in the health care industry.

Scientists and entrepreneurs are striving to bring ultra-sophisticated medical device software products to market. The coming generation of medical software will provide incredibly detailed images of human tissues, compounds, and molecules. In the very near future, health care facilities and medical practitioners will regularly transmit three-dimensional digital maps of patient tissues, compounds, and molecules over the wired and wireless Internet.[6] Since loss, alteration, corruption or misuse of a portion of that data is inevitable, patient injury is also inevitable. Thus, the legal responsibility for the loss, alteration, corruption, or misuse of patient data will soon be a matter for the courts.

This article provides an overview of federal regulatory law, intellectual property law, and negligence/products liability law that will govern the marketing of medical device software in the United States. This article then suggests an approach to address the primary business risks that holders of medical software intellectual

---

[4] U.S. Nuclear Regulatory Commission, Computer Codes, *available at* http://www.nrc.gov/what-we-do/regulatory/research/comp-codes.html (last visited Apr. 15, 2003).

[5] *See* Rear Admiral Kenneth D. Slaght, Remarks Before the Subcommittee on Research and Development of the House Armed Services Committee on Navy Transformation (Feb. 20, 2002), *at* http://chinfo.navy.mil/navpalib/testimony/research/kdslaght020220.txt (describing how FORCEnet, the Navy's transformational architecture linking Navy and Marine Corps and Allied and coalition forces, will be integrated with the Department of Defense Global Information Grid).

[6] *See* National Institute of Health, *National Library of Medicine to Unveil Vast Potential of Internet2 for Improving Delivery of Health Care* (Nov. 29, 2002), *available at* http://www.nih.gov/news/pr/nov2002/index.htm (last visited Apr. 15, 2003); IBM Life Sciences Solutions, *National Digital Mammography Archive: University of Pennsylvania Consortium and IBM Develop Computing Grid for Breast Cancer Screening, at* http://www-3.ibm.com/software/success/cssdb.nsf/CS/DGUN-5B2Q35?. For example, a University of Pennsylvania consortium funded by grants from the National Science Foundation, the National Library of Medicine, the National Institutes of Health, and Next Generation Internet are working with IBM to develop the National Digital Mammography Archive (NDMA). *Id.* The effort, to be completed in 2003, is to develop an Electronic Medical Record data grid and digital repository so that the full range of a patient's healthcare files including high fidelity medical images (CT, MRI, mammograms), records and clinical history could be stored an housed in networked data systems allowing the management and fast retrieval of huge files; digital mammograms typically consume 160 Mb of storage per study per patient. *Id.*; *see also* Douglas Page, *Universities Prepare National Digital Mammography Archive*, PACS WEB, *at* http://www.diagnosticimaging.com/pacsweb/stories/news04090101.shtml (last visited Apr. 15, 2003); National Digital Mammography Archive, *Project Overview, at* http://nscp01.physics.upenn.edu/ndma/projovw.htm (last visited Apr. 15, 2003).

property rights, medical software designers, businesses intent on marketing medical device software, and businesses intent on marketing medical devices that integrate or imbed medical software, will encounter in their business operations.

I. THE SETTING

You are fortunate to serve as counsel to a venture intent on marketing a long-sought advance in medical device technology that employs software to analyze digital representations of energy waves interacting with tissues, compounds and molecules deep within the human body. The software can create patient tissue maps and compare them with maps of known disease patterns, electronically store the data for long-term use, and electronically transmit the data.[7]

Your clients are a delight. As scientific-entrepreneurs, they are among the most competent and dynamic individuals in society.[8] As medical professionals they focus their talents and research to improve the well being of mankind. As capitalists, they encourage those with whom they deal to share in the risks and rewards: they offer you founders' shares in the new venture in exchange for your counsel and continued service.[9]

The new venture has invested large sums and thousands of hours developing the new technology, creating and refining a strategic business plan for its commercialization, and cultivating an intricate web of relationships with the physicians, technologists, researchers, business executives, and venture capitalists to market the new technology.[10]

The venture's chief medical scientist believes the technology has the potential to harness decades of painstaking research in a fundamentally new way. He states that the technology could change the practice of medicine and improve untold numbers of lives. He declares his intention to see the technology through delivery to the market.

The venture's lead software engineer matter-of-factly states that because of accelerating advances in computing technology, the new integrated medical device can be assembled from a mixture of technologies, old and new, including:

---

[7] The Food and Drug Administration online Manufacturer and User Facility Device Experience Database (MAUDE) includes a variety of entries disclosing the extent to which a number of manufacturers are seeking FDA Pre-Market Approval to manufacture these types of devices.

[8] *See* Lisa Spefchman, *Coleman's Bright Idea: How One Scientists Took on 14 Major Electronics Companies for Infringement and Won,* AMERICAN LAWYER MEDIA'S LAW.COM (September 9, 2002), *at* http://www.law.com/index.shtml/ (last visited Apr. 15, 2003).

[9] *See* Debra Baker, *Who Wants to be a Millionaire?: Law Firms Investing in Hot High-Tech IPOs are Making a Fortune, but Some Critics Worry the Stock Craze is Clouding Ethics Matters*, 86 A.B.A.J. 36 (2000). In rosier days, Wilson Sonsini Goodrich & Rosati acquired 102,584 shares of VA Linux, its client's stock, in exchange for legal services. *Id.* At the close of the first day of public trading, the shares were valued at $24.5 million. *Id.*

[10] *See* Paul A. Mathew, *Entrepreneurship, Technology, and Law at the University of Washington*, CENTER FOR ADV. STUDY & RES. IN INTELL. PROP. NEWSL., Vol. 9, Issue I, (2002), *at* http://www.law.washington.edu/Casrip/newsletter/newsv9i1Mathew.pdf (last visited Apr. 15, 2003).

* Off-the-shelf "pulse emitters" and "pulse recorders" that record very subtle changes in energy waves when the waves interact with human tissue;

* An off-the-shelf "converter" microprocessor that converts the signal structures of the energy waves into electronic digital format;

* An off-the-shelf "digitizer" that creates a three-dimensional depiction of the tissues studied;

* A new software program that analyzes the depictions of tissues for minute fluctuations during the testing process;[11]

* An off-the-shelf storage device that stores the depictions of tested tissue and healthy tissue;

* An off-the-shelf personal computer;

* An off-the-shelf operating system;

* An off-the-shelf communications program;

* An off-the-shelf compression program; and

* An off-the-shelf Internet communications program.

The venture's business executives enthusiastically detail the significant commercial and diagnostic advantages the new integrated device offers: it can be used to diagnose disease states far sooner then conventional technology; the use of the technology produces few or no harmful side effects to patients or health care professionals; the new equipment can be manufactured, distributed, serviced and maintained at a fraction of the cost of existing equipment; and the performance of the new equipment will improve as the new software is further refined and matures.

You suppress an inner shudder as your mind flashes through the events of the past two years. As a result of the multi-trillion dollar "telecom" and "dot-gone" financial debacles, the collapse of share prices of many leading technology companies, the aftermath of "9-11," the revelation of widespread "Enron/Arthur Anderson"

---

[11] The scientific medical community has been working at fever pitch to create the scientific standards and protocols necessary for the transfer of digitized medical imaging data. *See generally* Marcela Hernandez-Hoyos et al., *Computer-assisted Analysis of Three-Dimensional Magnetic Resonance Angiograms,* RADIOGRAPHICS, 22:421-436 (2002); Usha Sinha & Hooshang Kangarloo, *Principal Component Analysis for Content-based Image Retrieval,* RADIOGRAPHICS, 22:1271-1289 (2002); Bharti Temkin et al., *Web-based Three-dimensional Virtual Body Structures,* J. AM. MED. INFORMATICS. ASS'N, 9:425-436 (2002); Leo P. Lawler & Elliot K. Fishman, *Multi-Detector Row Computed Tomography of Thoracic Disease with Emphasis on 3D Volume Rendering and Computed Tomography Angiography,* RADIOGRAPHICS, 21:1257-1273 (2001).

corporate accounting fraud, and new federal corporate laws, the venture capital environment has been radically transformed.

As a result, venture capitalists (VC's) are requiring new technology ventures to carry the economic and psychological baggage of the recent past. Venture capital investment in new companies is only about 15% of what is was one year ago. Term sheets are very difficult to come by, and valuations are extremely low.[12] For only the second time in memory, VC's as a group recently returned more capital to their investors than they obtained from them.[13]

As a reflection of the maturation of the computer software industry, the mass adoption of computing technology by the health care industry,[14] and the documented risk of death or injury associated with the use of medical software, the Food and Drug Administration (FDA) has put into place a new regulatory framework that subjects medical device software to life-cycle scrutiny. Pursuant to Congressional mandate, the United States Department of Health and Human Services (HHS) is in the process of publishing regulations that will be used to govern the accessibility, security, and privacy of "individually identifiable health care information."

Medical device tort liability is recognized throughout the United States. A single "death case" now equates with ten-figure liability. Death and severe personal injury arising from the malfunction of medical device software is a documented reality.

Should the venture's new medical software obtain conditional FDA approval and enter the health care market, the inevitable failure of the medical software will lead the venture, the creator of the medical software program, the manufacturer of associated medical devices, and the holder of the intellectual property rights in the software program, to an encounter with the law of negligence and products liability.

There you stand, near the center of a high-risk, high-value, high-benefit entrepreneurial endeavor. The new medical technology may improve the quality of life for countless patients. Decades of scientific research will be subject to intense

---

[12] *See* Tricia Duryee, *VC Swoon Hurts Startups*, SEATTLE TIMES, Oct. 29, 2002 *available at* 2002 WL 3919685. On a national scale, fewer companies received first round venture capital investment in the third quarter than in any quarter in the past eight years. *Id.*; *see also* Tricia Duryee, *Venture Capitalists Reduce Stake in Washington Firms: 50 Percent Drop Seen From Last Quarter*, SEATTLE TIMES, Oct. 26, 2002, *available at* 2002 WL 3919236; Luke Timmerman, *Biotech's On Edge as Money Evaporates: Local Firms Resort to Reserves, Layoffs*, SEATTLE TIMES, Aug. 19, 2002, *available at* 2002 WL 3910238.

[13] *See Venture Capitalist Gave More Than They Got in the 2nd Quarter*, WALL ST. J., Aug. 6, 2002, *available at* 2002 WL-WSJ 3402718.

[14] *See generally* James S. Benson, *Forces Reshaping the Performance and Contribution of the U.S. Medical Device Industry*, 51 FOOD DRUG COSM. L.J. 189 (1997); Dee Simmons, *Medical Device Software Regulation: An Industry Perspective*, 51 FOOD DRUG COSM. L.J. 189 (1997). Leading medical device manufacturers are marketing a variety of new medical imaging software of the type contemplated by this article. *See, e.g.*, GE Systems Medical, *GE Medical Systems Announces Latest Molecular Medicine Initiatives*, News Releases (Nov. 6, 2002), *available at* www.gemedicalsystems.com/company/pressroom/releases/pr_release_7622.html; IBM, *Medical Imaging Solutions, Innovative IT Infrastructure Solutions for the Next Generation of Medicine*, IBM LIFE SCIENCES (December 3, 2002) *available at* http://www-3.ibm.com/solutions/lifesciences/solutions/medical.html.

federal regulatory scrutiny. Academic standing and professional careers are on the line. Staged investments in the tens of millions of dollars loom ahead.

Your clients ask whether you can help them structure operations of the venture to reflect the venture's federal regulatory, intellectual property, and tort liability concerns. Your advice, Counselor?

II. THE FEDERAL REGULATORY LANDSCAPE

A. Food and Drug Administration Regulation of Medical Software

The FDA is broadly empowered to regulate the use of medical devices pursuant to section 201(h) of the Federal Food, Drug, and Cosmetic Act.[15] A regulated "medical device" is defined as:

> [A]n instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or related article, including any component, part or accessory, which is:
>
> (1) recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;
>
> (2) intended for use in the diagnosis of disease, or other conditions, or in the cure, mitigation, treatment or prevention of disease, in man;
>
> (3) intended to affect the structure or any function of the body of man . . . which does not achieve its primary intended purposes through chemical action within or on the body of man . . . and which is not dependent upon being metabolized for the achievement of its primary intended purposes.[16]

---

[15] *See* 21 U.S.C. § 321 (2000 & Supp. 2003). The FDA has comprehensive regulatory power over a vast array of products sold in interstate commerce. *Id.* The FDA regulates biologics (safety of the blood supply), cosmetics, drugs, electronic products (such as radiation safety performance standards, diagnostic x-ray equipment, laser products, and ultrasonic therapy equipment), foods, medical devices (involving pre-market approval of new devices, manufacturing and performance standards, and tracking reports of device malfunctioning and serious adverse reactions), and veterinary products. *Id.* The data base system that tracks the nation's blood supply is a regulated "medical device". *Id.*

[16] 21 U.S.C. § 321 (2000 & Supp. 2003). A disposable, wooden tongue depressor is a Class One regulated "medical device." *Id.* at § 360(c). It is a simple device, involves low risk of harm to the patient or the care giver, receives an administrative review of the labeling used to describe it, and likely has no significant difference in technology or characteristics from other tongue depressors used by the medical profession for the past 100 years. *See id.* The medical software device envisioned in this article would probably be classified as a Class Three regulated "medical device." *See id.* It would be a complex device that could present a high degree of risk to the patient were it to

Pursuant to the Federal Food, Drug, and Cosmetic Act, any software product meeting the definition of a "medical device" is subject to regulation by the FDA.[17] The FDA regulates stand-alone software devices for which the software is not an accessory to another device,[18] any software accessory to a medical device that accepts data and modifies it for input to a medical device, and any software that takes data from a medical device and modifies if for presentation to the user.[19] Components, parts, or accessories to a classified device are regulated like the parent device.[20]

The FDA's new software regulatory framework is the result of two decades of experience with the use of computer software in medical device technology.[21] The policy has unfolded against a backdrop of the new Quality System Regulation for medical devices,[22] and the enactment of the Food and Drug Administration Modernization Act of 1997.[23]

The new FDA medical device software regulatory framework is based on the following premises:

* Software products meet the definition of medical devices and are regulated as such, unless specifically exempted;

* The FDA uses a risk-based approach to regulation;

* The FDA will use the least amount of regulatory control necessary to regulate risk;

---

provide incomplete or inaccurate diagnostic information. Additionally, the FDA has had little or no experience with the safety and effectiveness of the device, and it would be subject to pre-market approval and a comprehensive review by a team of experts. *See generally* Michael D. Green & William B. Schultz, *Tort Law Deference to FDA Regulation of Medical Devices*, 88 GEO. L.J. 2119 (2000).

[17] *See* E. Stewart Crumpler & Harvey Rudolph, *FDA Software Policy and Regulation of Medical Device Software*, 52 FOOD DRUG COSM. L.J. 511, 512 (1997) (calling for comment on prospective FDA computer software policy by senior FDA regulatory personnel).

[18] *Id.* Regulated stand-alone medical software devices include pharmacy prescription ordering systems, laboratory information management systems, blood establishment information management systems and expert medical decision support systems. *Id.*

[19] *Id.* Regulated accessory software devices include radiation treatment planning software, digital imaging and image conversion software, picture archiving and communication systems, and EEG and ECG waveform analysis software. *Id.*

[20] *Id.* at 513.

[21] *Id.* at 514-15. The first FDA medical software policy statement was issued in draft form in 1989. *FDA Policy for Regulation of Computer Products, Draft*, Food and Drug Administration, Center for Devices and Radiological Health (1989), *available at* http://www.fda.gov/cdrh/ode/351.pdf (last visited Apr. 15, 2003). The draft statement had no legal status, caused industry confusion, and lead to the consumption of limited FDA resources in time consuming case-by-case determinations. *See* Crumpler & Rudolph, *supra* note 17, at 514-15.

[22] *See* 21 C.F.R. § 820.3 (1996).

[23] Larry R. Pilot & Daniel R. Waldman, *Food and Drug Administration Modernization Act of 1997: Medical Device Provisions*, 53 FOOD DRUG COSM. L. J. 267, 267-68 (1998).

* The FDA requires the use of design controls, independent audits, and the identification of appropriate software standards;

* Low-risk software devices have the least amount of control and will be granted exemption from all regulatory requirements excepting misbranding;

* Moderate-risk software devices may qualify for less stringent 510(k) "substantial equivalent" application review;

* High-risk software devices shall be subject to very rigorous pre-market approval review.[24]

Three final FDA Guidance documents regulate medical devices that incorporate or imbed medical software:

* "Guidance for the Content of PreMarket Submissions for Software Contained in Medical Devices;"[25]

* "Off-the-Shelf Software Use in Medical Devices;"[26]

* "General Principles of Software Validation; and Final Guidance for Industry and FDA Staff."[27]

1. Overview of "Guidance for the Content of PreMarket Submissions for Software Contained in Medical Devices"

PreMarket Submissions provides a framework of software programming means that must be used to obtain FDA approval to market medical device equipment.[28] PreMarket Submissions is applicable to all types of medical devices containing software for which applicants file pre-market notifications (510(k)'s), Pre-market Applications, Investigational Device Exemptions, and Humanitarian Device

---

[24] *See* Crumpler & Rudolph, *supra* note 17, at 514.

[25] Center for Devices & Radiological Health, *Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, U.S. Food & Drug Administration (May 29, 1998), *available at* http://www.fda.gov/cdrh/ode/57.html [hereinafter *Premarket Submissions*].

[26] Center for Devices & Radiological Health, *Guidance for Industry*, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices, U.S. Food & Drug Administration (August 17, 1998), *available at* http://www.fda.gov/cdrh/ode/guidance/585.html [hereinafter *Off-The-Shelf Software*].

[27] Center for Devices & Radiological Health, *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*, U.S. Food and Drug Administration (January 11, 2002), *available at* http://www.fda.gov/cdrh/comp/guidance/938.html [hereinafter *Final Guidance*].

[28] *Premarket Submissions*, supra note 25, at § 1.3.

Exemptions.[29] Appendix B to PreMarket Submissions lists sixty-seven national and international consensus standards, grouped by relevant class, that are to be viewed as tools for achieving and demonstrating compliance with the FDA medical software standard.[30] Appendix C contains an extensive bibliography of leading treatises and guidance standards materials.[31]

PreMarket Submissions uses the term "level of concern" to serve as a baseline estimate of the severity of injury that a device could permit or inflict, directly or indirectly, on a patient or operator because of a latent failure or design flaw encountered during the medical use of medical device software. The extent of the pre-market review process pertaining to software products is proportional to the level of concern. Manufacturers are asked to specify the level of concern for the software product and describe how the level of concern was determined. The level of concern for medical device software varies over a continuum.[32]

PreMarket Submissions requires that the severity of the hazard resulting from the failure of the software be characterized assuming that software failure *shall* occur.[33] Software failures are deemed to be systemic in nature; the probability of their occurrence cannot be determined in advance using traditional statistical methods.

PreMarket Submissions establishes three levels of concern: major, moderate or minor. A major level of concern is present when failure of the software product could result in incorrect or delayed information that could cause the death or serious injury of the patient, the operator, or both. A moderate level of concern is present when failure of the software product could result in incorrect or delayed information that could cause non-serious injury of the patient, the operator, or both. A minor level of concern is present when failure of the software product would not be expected to result in injury to the patient or operator. The interrelationships of the three levels of concern are analyzed in flow chart sequence.[34]

Section Three of PreMarket Submissions sets forth the minimum types and qualities of documentation needed to support FDA pre-market approval for medical device software. To gain approval for medical device software involving a major level of concern, the applicant must submit detailed documentation for each of the following criteria:

---

[29] *Id.*

[30] *Id.* at Appendix B. American National Standards Institute (ANS) and Institute of Electrical and Electronic Engineers, Inc. (IEEE) standards are segregated into eight classes: General Life Cycle Activities; Safety and Reliability; Quality Assurance; Configuration Management; Test and Evaluation; Automated Tools; and Human Factors Engineering; s*ee generally* Anthony L. Young, *An Overview of ISO 9000 Application to Drug, Medical Device, and Environmental Management Issues*, 49 FOOD DRUG COSM. L.J. 469 (1994).

[31] *Premarket Submissions, supra* note 25, at Appendix C.

[32] *Id.* at § 2.2.

[33] *Id.* at § 2.2.1. A "serious injury" is defined as an injury or illness that is life threatening, results in permanent impairment of a body function or permanent damage to a body structure, or necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure. *Id.*; 21 C.F.R. § 803.3 (2003).

[34] *Premarket Submissions, supra* note 25, at § 2.2.1, Fig. 2.

* Level of Concern - the level of concern and supporting rationale;

* Software Description - a comprehensive overview of the medical device features that are controlled by the software;

* Device Features Controlled by Software - the role of the software in the device, how the user interfaces with the software, which software features can be modified by the user, and hardware over-rides or backups;

* Operational Environment - the programming language, hardware platform, operating system, and Off-the-Shelf components;

* Device Hazard Analysis - all device hazards associated with the intended use, hardware and software;

* Software Requirements Specification - functional, performance, interface, design and developmental requirements;

* Architecture Design Chart - the partitioning of the software into its functional subsystems, a list of functional modules, and a description of the role each module plays in the fulfilling the software requirements;

* Design Specification - a high-level summary of the design and specifications detailed enough such that a programmer is not required to make ad hoc decisions;

* Traceability Analysis - a matrix linking requirements, design specifications, hazards and validation;

* Development - the processes that are in place to manage the software development life cycle, an annotated list of baseline documents, and the configuration management and maintenance plan;

* Validation, Verification and Testing - a description of the verification activities at the unit, integration and system level, and unit, integration and system level test protocols including pass/fail criteria, test report, summary and test results;

* Revision Level History - the revision log documenting all major changes to the software during its development cycle;

* Unresolved Anomalies (Bugs) - each anomaly, the problem, the impact on device performance, how they affect safety or effectiveness, and any plans or timeframes for correcting the problem;

* Release Version Number - the release version number and date for the software that will be included in the marketed device.[35]

To gain conditional pre-market approval to market major risk medical software, the applicant must submit documentation to FDA describing ongoing risk management, hazard analysis, risk estimation, risk control, and life-cycle risk management activities. For each identified hazard, the applicant must identify the risk control method used to eliminate the risk or reduce the risk to an acceptable level, as well as the severity level after risk control methods have been implemented. The goal is to reduce all software-related hazards to a minor level of concern.[36]

2. Overview of "Off-the-Shelf Software Used In Medical Devices"

FDA regulation of the use of Off-the-Shelf Software (OTS software) in medical devices is based on the assumption that OTS software intended for general purpose computing may not be appropriate for use in a medical device. OTS software components are rapidly obsolete, they are easily changeable, and they are typically not supported for long periods.[37]

The type and amount of documentation to be provided to FDA on the use of OTS medical software increases with the severity of the hazards to patients, operators, or bystanders arising from the failure of OTS software.[38] The regulation of OTS software reflects a safety-based approach to risk management consistent with international standards of risk management.[39]

Applicants must provide a variety of basic documentation for each OTS software component used in the applicant's medical device. The documentation must include:

* An exact identification of the OTS software;

* The computer system specifications for the OTS software;

---

[35] *Id.* at § 3.0. FDA premarket approval for sophisticated medical device software reaches all of the components of software driven medical devices. *Id.* at § 1.3. *See, e.g.,* CTR. FOR DEVICES AND RADIOLOGICAL HEALTH, U.S. FOOD AND DRUG ADMIN., PREMARKET APPROVALS (Apr. 2002), http://www.fda.gov/cdrh/pma/pmaapr02.html (FDA approval of protocol to for review of Image Analysis system to be marketed by R2 Technology); CTR. FOR DEVICES AND RADIOLOGICAL HEALTH, U.S. FOOD AND DRUG ADMIN., PREMARKET APPROVALS (Feb. 1997), http://www.fda.gov/cdrh/pmafeb97.html (FDA approval granted for changes to the computer system and operator's manual for deep heating ultrasound system to be marketed by Labthermics Technologies, Inc.); CTR. FOR DEVICES AND RADIOLOGICAL HEALTH, U.S. FOOD AND DRUG ADMIN., PREMARKET APPROVALS (Jan. 2002), http://www.fda.gov/cdrh/pma/pmajan00.html (FDA approval of design changes consisting of the integration of data controller and associated software, the replacement of a cubaclinical serial connector, and data controller operating instructions for a bone sonometer to be marketed by McCue PLC).

[36] *Premarket Submissions, supra* note 25, at § 4.3.2.

[37] *Off-The-Shelf Software, supra* note 26, at § 1.1.

[38] *Id.*

[39] *Id.* at § 1.2.

* A statement describing the function of the OTS software;

* A statement describing the testing, verification and validation of the OTS software for use with the applicant's medical device;

* A statement describing how the applicant will insure the proper use of the OTS software by End Users.[40]

The applicant must also submit a software hazard analysis and a software hazard mitigation analysis, and he or she must justify all residual risks associated with the use of OTS software.[41] Should the OTS software itself represent a major level of concern, the applicant must provide assurance to the FDA that the product development methods used by the OTS software developer were sufficient to support the secondary use of the OTS software in the applicant's device.

The FDA specifically warns that if the applicant is unable to properly audit the OTS software developer's software design and development methodologies and cannot properly mitigate all related hazards, the use of the OTS software is *not* appropriate for the intended application. The applicant must take steps to assure the FDA that the original developer will maintain the OTS software or establish escrow arrangements to insure continued access to the OTS software code.[42]

3. Overview of "General Principles of Software Validation"

Software Validation requires medical software developers to determine the proper integration of software life cycle risk management activities, to document the use of the proper programming approach, to describe the combination of software engineering techniques to be used, and to indicate the level of support to be provided to the medical software product.[43]

Software Validation sets forth a new operational parameter for medical software in that medical software must be "validated." Validation is "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled."[44] Validation is the process by which the medical device software provider demonstrates "a level of confidence before shipping the product that the device meets all requirements and user expectations for the software automated functions and features of the device."[45]

The FDA's "software validation" standard is based on these criteria:

---

[40] *Id.* at § 2.1.
[41] *Id.* at §§ 2.2-2.4.
[42] *Id.* at § 2.5.
[43] *Final Guidance, supra* note 27, at § 2.4.
[44] *Id.* at § 3.1.2.
[45] *Id.*

* Due to its complexity, the development process for software should be more tightly controlled than the development process for hardware;

* The quality of software product is dependent primarily on design and development with a minimum of concern for manufacture;

* The ability of programs to execute alternative series of commands based on differing inputs, "branching," makes programs complex and difficult to understand;

* Testing alone cannot verify that software is complete and correct;

* Although software may improve with age as latent defects are discovered and removed, new defects can be introduced into software as updates are issued;

* Software failures occur without advance warning;

* Insignificant changes in software code can create unexpected and significant problems elsewhere in the program;

* Software maintenance personnel are not typically those involved in the original software development effort;

* Time is needed to fully define and develop reusable software code and understand the behavior of off-the-shelf components.[46]

Software Validation includes a lengthy section describing a variety of life cycle activities that "support a conclusion that software is validated."[47] The new regulations reach the very heart of medical software code.

To support a conclusion that a piece of medical device software has been validated, the FDA may require the applicant to provide detailed documentation demonstrating compliance with a host of software engineering, coding, testing and maintenance activities, including:

* Quality planning, requirements specification, design, construction or coding, testing by the software developer, user site testing, and maintenance and software changes;[48]

* Software risk analysis, traceability analysis, software design evaluation, design communication link analysis, module test plan

---

[46] *Id.* at § 3.3.
[47] *Id.* at § 5.
[48] *Id.*

generation, integration test plan generation, and test plan generation;[49]

* Statement coverage, branch coverage, condition coverage, multi-condition coverage, loop coverage, path coverage, and data flow coverage;[50]

* Module or component level testing, integration level testing, and system level testing;[51]

* Anomaly (bug) evaluation, problem identification and resolution tracking, proposed change assessment, task iteration, and documentation updating.[52]

Software Validation closes with a massive bibliography that identifies eleven FDA References, thirteen "Other Government References," nineteen "International and National Consensus Standards," seven "Production Process Software References," and forty-eight "General Software Quality References."[53]

B. Health and Human Services Regulation of Medical Software

HHS is empowered to regulate the use of "health information" pursuant to the Health Insurance Portability and Accountability Act.[54] HHS is about to publish final regulations governing the electronic transmission of health information.[55] Health information is defined as:

---

[49] *Id.* at § 5.2.3.

[50] *Id.* at § 5.2.5. Techniques exist to determine what percentage of a software program has been structurally evaluated. *Id.* If a testing program determines that a software program has achieved "statement coverage," 100% of the statements in the software have been executed at least once. *Id.*

[51] *Id.* at § 5.2.6.

[52] *Id.* at § 5.2.7.

[53] *Id.* at Appendix A.

[54] Health Insurance Portability & Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[55] For a look at the evolution of proposed rules applicable to electronic transactions, see The Health Care Financing Administration, *Security and Electronic Signature Stands: Proposed Rule*, U.S. Department of Health & Human Services (Aug. 12, 1998). 45 C.F.R. § 142 (1998). Portions of the proposed rule applicable to eight types of electronic transactions now appear in *Health Insurance Reform: Standards for Electronic Transactions*, 45 C.F.R. §§ 160, 162 (1998). Publication of the remaining portions of the proposed rule are pending. *Id.* The regulations are intended to establish a flexible, scalable approach that requires organizations wishing to conduct electronic exchanges of medical information to implement necessary measures to protect the confidentiality and integrity of the data exchanged. *Id.* Portions of the proposed rule became effective in October, 2002 for health care clearinghouses and health care providers that choose to transmit any of the transactions in electronic form. An effective date of October, 2003, was enacted for small health care plans. *Id.; see* U.S. Department of Health and Human Resources, *Frequently Asked Questions About Electronic Transaction Standards Adopted Under HIPAA, available at*

> [A]ny information, whether oral or recorded in any form or medium that -Is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
>
> Relates to the past, present, or future physical or mental health or condition of the individual; the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[56]

The HHS regulation will govern the enormous volume of health information generated by the American health care industry in various ways, including:

* "Group health plans"[57] having 50 or more "participants" or those administered by an entity other than the employer that established and maintains the plan;[58]

* "Health insurance issuers"[59] including insurance companies and businesses providing services to insurance organizations licensed to engage in the business of insurance in a State and are subject to State law regulating insurance;[60]

* "Health maintenance organizations;"[61]

* Part A or Part B of the Medicare program;[62]

* The Medicaid program;[63]

---

aspe.hhs.gov/adminsimp/faqtx.htm (last visited April 15, 2003); U.S. Department of Health and Human Resources *What are the Major Differences Between the Proposed Rule and the Final Rule, available at* aspe.hhs.gov/adminsimp/faqtxdif.htm (last visited April 15, 2003); *see also* Health Insurance Reform, Security Standards, 45 Fed. Reg. 8334-01 (Feb. 20, 2003) (to be codified at 21 C.F.R. §§160, 162 and 164). This final rule adopts standards for the security of electronically protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. *Id.* The use of the security standards will improve the Medicare and Medicaid programs and other federal and private health programs, as well as the effectiveness and efficiency of the health care industry in general, by establishing a level of protection for certain electronic health information. *Id.*

[56] Health Insurance Portability & Accountability Act, Pub. L. No. 104-191, § 1171(4), 110 Stat. 1936, 2022 (1996).

[57] *See* 42 U.S.C. § 300gg-91(a)(1) (2000).

[58] *See generally* Employee Retirement Income Security Act, Pub. L. No. 93-406, 88 Stat. 829 (1974) (codified as amended at 29 U.S.C. §§ 1001-1461 (2000)).

[59] *See* 42 U.S.C. § 300gg-91(b)(2) (2000) (defining "Health Insurance Issuers").

[60] *Id.*

[61] *See* 42 U.S.C. § 300gg-91(b)(3) (2000) (defining "Health Maintenance Organization").

[62] *See* 42 U.S.C. § 1395 (2000).

[63] *See* 42 U.S.C. § 1396.

* Medicare supplemental policies;[64]

* The health care program for active military personnel;[65]

* The veterans health care program;[66]

* The Federal Employees Benefits Program.[67]

* "Any other individual or group health plan or combination that provides or pays for the cost of medical care."[68]

The HHS regulation specifically applies to "individually identifiable health information," defined as:

"[I]nformation that ---

a. is created or received by a health care provider, health plan, employer, or health clearinghouse; and

b. relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

i. identifies the individual, or

ii. with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[69]

The electronic exchange of "individually identifiable health information" between two parties to "carry out financial and administrative activities related to health care" will constitute a "regulated transaction."[70] Regulated transactions shall

---

[64] *See* 42 U.S.C. § 1882(g)(1) (2000). A "Medicare supplemental policy" is a health insurance policy that a private entity offers to a Medicare beneficiary to provide payment for expenses incurred for services and items that are not reimbursed by Medicare. *Id.*

[65] *See* 10 U.S.C. § 1074 (2000).

[66] *See* 38 U.S.C §§ 1101-2411(2000).

[67] *See* 5 U.S.C. § 8901 (2000).

[68] *See* Security and Electronic Signature Standards, 63 Fed. Reg. 43241-80 (proposed Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142), *available at* http://www.hipaadvisory.com/regs/Regs_in_PDF/security_electronic_sign_stand.pdf.

[69] *See* 42 U.S.C. § 1171(6) (2000).

[70] *See* 42 U.S.C. § 1173(a)(2).

include the electronic exchange of "First Report of Injury" data[71] and "Health Claims Attachment" data.[72]

III. THE INTELLECTUAL PROPERTY LANDSCAPE

A. Software Programs and Trade Secret/Unfair Competition Law

Most states grant computer software trade secret protection pursuant to the Uniform Trade Secrets Act or the *Restatement (Third) of Unfair Competition*. The Uniform Trade Secrets Act defines a trade secret as information, including any formula, pattern, compilation program, device or process, which derives independent value from not being generally known and which is the subject of reasonable efforts to maintain its secrecy.[73] The *Restatement of Unfair Competition § 39* defines a trade secret as any formula, pattern, device or compilation of information that is used in one's business that provides opportunity or advantage over competitors who do not know or use it.[74]

Trade secret protection extends to ideas and processes contained in software programs, as well as to the specific expressions of them. Protection does not depend on novelty or uniqueness. So long as secrecy is maintained, protection continues in perpetuity.

Software programming information may qualify for trade secret protection, depending on: the degree to which the information is known outside the programmer's business; the extent to which the information is known by employees and others involved in the business; the measures taken to maintain secrecy of the information; the value of the information; the amount of effort or money used to develop the information; and the degree of difficulty required by others to properly acquire the information.[75]

Trade secret protection is premised on proof of "misappropriation." Protection extends only insofar as a plaintiff can prove that the defendant's access to the plaintiff's trade secrets was the result of an improper abuse of a confidential relationship between them.[76] Once a product is made available to the general public, competitors can lawfully attempt to discern trade secrets built into software by

---

[71] *See* Security and Electronic Signature Standards, 63 Fed. Reg. at 43248. "First Report of Injury Transactions" may report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims and risk management requirements. *Id.*

[72] *Id.* at 43265. Health claims attachments may report information used to transmit health service information, such as subscriber, patient, demographic, diagnosis, or treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a health services review. *Id.*

[73] UNIFORM TRADE SECRETS ACT § 1(4) (1985).

[74] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). This definition is based upon the RESTATEMENT OF TORTS § 757 (1939).

[75] *See* RESTATEMENT (THIRD) OF TORTS § 757 (1998).

[76] UNIFORM TRADE SECRETS ACT at § 1(2) (1985).

reverse engineering, copying, or using the software.[77] A party who misappropriates trade secret information may not lawfully use the information for commercial gain.[78] As the term implies, trade secrets need not be recorded or registered with third parties, as disclosure would strip away the secrecy component.

Pursuant to the Uniform Trade Secrets Act, a plaintiff must prove that he took "reasonable measures" to protect the secrecy of the information.[79] What constitutes reasonable measures is a factual question balancing an estimation of the costs and benefits of varying levels of protection by persons knowledgeable in the particular field.[80] The more the owner of the trade secret spends to protect the information, the more he demonstrates that the secret has real value deserving of legal protection, that he was hurt by result of misappropriation of it, and that misappropriation occurred.[81] The use of non-disclosure agreements is considered to determine whether plaintiff acted reasonably.

Third parties are not precluded from independently discovering and using trade secrets held by others. Should a third party independently discover the trade secrets of another, the third party may obtain a patent in the discovery and exclude the original inventor from using, marketing, or licensing the former trade secret.[82]

Once a trade secret enters the public domain, the law will not restrict the subsequent use of the underlying information by third parties. The holder of a former trade secret may seek damages from or injunctive relief against the person or entity that misappropriated the former trade secret. The courts will probably not issue injunctive relief restraining subsequent dissemination of former trade secret information on First Amendment grounds.[83]

B. Software Programs and Copyright Law

Copyright protection is granted to original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced or otherwise communicated.[84] Copyright does not protect ideas, processes, or methods of operation.[85] The Copyright Act has been amended to include a definition of a computer program as "a set of statements or instruction to be used directly or indirectly in a computer in order to bring about a certain result."[86]

---

[77] Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 155 (1989).

[78] *See e.g.* Speech Tech. Assoc. v. Adaptive Comm. Sys., Inc., 1994 U.S. Dist. LEXIS 11660, 26 (N.D. Cal. Aug. 16, 1994); DVD Copy Control Ass'n v. Bunner, 113 Cal.Rptr.2d 338 (6th App. Dist. 2001).

[79] Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174, 179 (7th Cir. 1991).

[80] *Id*

[81] *See id.*

[82] *See generally* W.L. Gore & Assoc., Inc. v. Garlock, Inc., 721 F.2d 1540, 1545 (Fed. Cir. 1983) (describing failed attempt by inventor of Gore-tex fabric manufacturing process to maintain trade secret protection over manufacturing process).

[83] DVD Copy Control Ass'n, 113 Cal.Rptr.2d at 340.

[84] 17 U.S.C. § 102(a) (2000).

[85] 17 U.S.C. § 102(b) (2000).

[86] 17 U.S.C. § 101 (2000).

Copyright protection extends only to the author's form of expression, not to the idea that was the basis of the author's expression.[87] That rationale flows from the decision of the Supreme Court in *Baker v. Selden*. The Court reasoned, "Copyright of a work on mathematical science cannot give to the author an exclusive right to methods of operation he propounds, or the diagrams which he employs to explain them."[88] Lower federal courts have limited the rule, reasoning that if there are only a finite number of ways to express an idea, the idea does not qualify for copyright protection.[89] Thus, where an idea and the expression of the idea become inseparable, the expression of the idea does not qualify for copyright protection.[90]

The courts have struggled to determine the boundaries of copyright protection of computer software programs. Non-literal elements of software have been given limited protection. A minority of courts follows the rule expressed in *Whelan Assoc. v. Jaslow Dental Labs., Inc.*, that extends copyright protection to the structure, sequence, and organization of a computer program.[91]

The majority of courts follow the complex "abstraction-filtration comparison test" devised by Judge Learned Hand in *Nichols v. Universal Pictures Corp.*[92] Judge Hand's test requires the court to segment programs on the basis of varying levels of abstraction. First, the general idea is identified; implementation of the idea in program sub-segments follows. Each of the sub-segments are tested to determine whether they may qualify for copyright protection. Segments of the program that can be expressed in no other way, segments dependent upon external factors, and segments in the public domain, do not qualify for copyright protection. The remainder of the program - the essence of programmer's creative expression - can obtain copyright protection.[93]

Under either test, substantial portions of software programs that contain material in the public domain or non-creative expression do not qualify for copyright protection. Specialized medical software programs containing new algorithms are much more likely to qualify for copyright protection than are programs in widespread general use.

The holder of the copyright is granted the exclusive right to make copies of the program, to prepare derivative works of the program, and to distribute copies of the program.[94] The copyright holder may not bar others from using similar programming

---

[87] 17 U.S.C. § 102(b) (2000).

[88] 101 U.S. 99 (1879).

[89] *See, e.g.,* Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 836 (10th Cir. 1993) (detailing the "idea-expression dichotomy" with respect to computer programs).

[90] *Id.* at 838. This idea is central to the merger doctrine, which allows for denial of copyright protection to an expression that relies upon underlying ideas, processes, or discoveries. *Id.*

[91] 797 F.2d 1222 (3d Cir. 1986).

[92] 45 F.2d 119, 121 (2d Cir. 1930) (explaining the need for consideration of abstractions with respect to a play, because "as more and more of the incidents are left out .... there is a point in this series of abstractions where they are no longer protected, since otherwise the playwright could prevent the use of his 'ideas,' to which, apart from their expression, his property is never extended.").

[93] *See* Computer Assoc. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 710 (2d Cir. 1992) (terming the leftover elements the "golden nugget" of the work's copyright value).

[94] 17 U.S.C. § 106 (2000).

techniques to achieve the same general result.[95] Unless prohibited by contractual terms, reverse engineering of a computer program is lawful so long as the effort is made to discover non-protected or non-protectable portions of the program.[96]

Once the program is fixed in a tangible medium copyright protection attaches automatically.[97] The term of protection is for the life of the author plus seventy years, or if the work was made for hire, for the first to expire of either seventy-five years from first publication or 100 years from creation.[98] Publication is not required.[99] Registration is required to bring an action for enforcement.[100]

C. Software Programs and Patent Law

1. Overview

The United States Constitution explicitly provides for the creation of patent rights[101] that confer a monopoly on the holder of the grant[102] for a limited term.[103] The invention must be a machine, article or manufacture, process, or composition of matter.[104]

If the patent owner can demonstrate to the satisfaction of the United States Patent and Trademark Office (PTO) that the invention is useful, novel, not a law of nature or science, and non-obvious to one reasonably skilled in the applicable art,[105] the PTO may issue a patent. Of particular importance, the applicant for a computer software patent must disclose the "best mode" of program operation; failure to disclose the "best mode" can constitute grounds for denial of a patent by the PTO or the issuance of a court order declaring a patent issued by the PTO invalid.[106]

---

[95] 17 U.S.C. § 102(b) (2000).

[96] *See* Sega Enters., Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527 (9th Cir. 1992).

[97] 17 U.S.C. § 102(a) (2000).

[98] 17 U.S.C. § 302 (2000).

[99] *Id.*

[100] 17 U.S.C. § 412 (2000).

[101] *See* U.S. CONST. art. I, § 8, cl. 8 ("[T]he Congress shall have the Power to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

[102] *See* 35 U.S.C. § 271 (2003). The patent owner may prohibit others from making, selling, or offering for sale the patented invention in the United States. *Id.*

[103] *See* 35 U.S.C. § 154(c)(1) (2003). For patents issued on or after June 8, 1995, the term of the patent is twenty years from the date of application. *Id.* For patents issued before June 8, 1995, the term is the longer of seventeen years from issue, or twenty years from date of filing. *Id.*

[104] 35 U.S.C. § 101 (2003).

[105] 35 U.S.C. §§ 101-03 (2003).

[106] *See, e.g.*, White Consol. Indus. v. Vega Servo Control, Inc., 713 F.2d 788 (Fed Cir. 1983).

2. Software Patents

For many years, the PTO refused to grant patents in software, holding that software was a set of mathematical equations and algorithms that, standing alone, were not new processes. The policy was changed in *Diamond v. Diehr*.[107] There, the United States Supreme Court held that a mathematical algorithm included in a software application could qualify for patent protection so long as the software application was part of a larger patentable process. Subsequent case law has firmly established patent protection for software.[108] Software patents have been granted for inventions governing system functions, as well as those involving the use of a mouse, speech recognition, and display functions.[109]

The PTO has issued guidelines governing the patentability of computer-implemented inventions.[110] The PTO guidelines state that a computer program is a "machine." Additionally, computer memory is defined as an article of manufacture, and a series of steps controlled by a computer is designated as a "process."[111]

Initially, the software industry did not seek software patents. The industry included many new ventures that did not wish to incur the expense of patent protection and that voiced opposition to software patents in general. Oracle Corporation publicized an official company policy opposing the patentability of software-related inventions.[112] In 1991, Microsoft owned ten United States patents. Reflecting the growth of the Internet and the liberalization of laws and policies governing the grant of software patents, the attitude of the industry has changed. By February 2002, Microsoft owned more than 2,000 U.S. patents. Oracle, patent-deprived through 1994, was known to hold to 249 patents in 2001.[113]

3. "Business Method" Software Patents

For many years, the courts routinely held that a patent should not be granted for "a system of transacting business disconnected from the means of carrying out the system."[114] Even the Patent and Trademark Office was unclear as to the status of business methods, stating that while they could fall within the method or process categories, they can none-the-less be rejected for lack of patentable subject matter.[115]

---

[107] 450 U.S. 175 (1981).

[108] *See, e.g., In re* Alappat, 33 F.3d 1526 (Fed. Cir. 1994) (holding that software program that created a smooth waveform suitable for display on a digital oscilloscope could be patented).

[109] *See* U.S. Pat. No. 5,443,068 (issued Aug. 22, 1995); U.S. Pat. No. 5,440,663 (issued Aug 22, 1995); U.S. Pat. No. 5,442,742 (issued Aug. 15, 1995); U.S. Pat. No. 5,394,546 (issued Feb. 25, 1995).

[110] Examination Guidelines for Computer-Implemented Inventions, 61 Fed. Reg. 7478 (Mar. 28, 1996).

[111] Examination Guidelines, 61 Fed. Reg. 7478 at ¶ IV.B.2(a)(ii).

[112] *Id.*; *see Oracle Company-Patent Policy, at* http://www.base.com/softwarepatents/statements/oracle.statement.html.

[113] T. Andrew Culbert, *Lecture on Legal Issues Concerning Software Patents* (Apr. 23, 2002).

[114] Hotel Security Checking Co. v. Lorraine Co., 167 F. 460, 469 (2d Cir. 1908).

[115] *See* State Street Bank & Trust Co. v. Signature Financial Group, Inc., 149 F.3d 1368 (Fed. Cir. 1998).

The Federal Circuit abolished the rule prohibiting the patentability of business methods in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*[116] Reasoning that "patentability does not turn on whether the claimed method does `business' instead of something else, but on whether the method viewed as a whole, meets the requirements of patentability," the court reversed a PTO holding denying a grant of patent for a software system used to manage a "hub and spokes" financial accounting structure.[117]

The combined effects of the changes in judicial and regulatory policy and the widespread adoption of the World Wide Web led to a rush on the PTO. Many businesses sought business method patents to capitalize on technologies developed for the commercialization of the Internet.[118]

It became apparent that the PTO had insufficient resources and technical expertise to deal with demand.[119] In response to concern about the quality and legal validity of business method patents, the PTO issued a Business Methods Patent Initiative.[120] The PTO dedicated itself to work more closely with software, Internet and electronic commerce ventures in order to enhance the technical training and expertise of patent examiners and to revise guidelines governing standards for patentability for computer-related inventions.[121]

At the same time, the courts began focusing on the legal sufficiency of business methods patents.[122] Relying on its newly issued "One-Click" e-commerce business method patent, Amazon.com attempted to enjoin similar e-commerce operations by BarnesAndNoble.com. Although the battle initially went Amazon's way, the Federal Circuit held that Barnes & Noble raised sufficient challenges to the validity of the Amazon "business method" patent that a trial on the merits was required.[123]

Measured against the backdrop of other significant patent policy matters,[124] the trend appears to be that business method software patents will be given close judicial scrutiny, and that business method patentees can expect serious challenge from alleged infringers.[125]

---

[116] *Id.*

[117] *Id.* at 1375.

[118] Culbert, *supra* note 113.

[119] *Id.*

[120] *Business Methods Patent Initiative: An Action Plan*, United States Patent and Trademark Office, *available at* http://www.uspto.gov/web/offices/com/sol/actionplan.html.

[121] *Id.*

[122] Culbert, *supra* note 113.

[123] Amazon.com, Inc. v. BarnesAndNoble.com, Inc., 239 F.3d 1343 (Fed. Cir. 2001).

[124] The Supreme Court, in *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722 (2002) (holding that there was a flexible estoppel bar rather than an absolute estoppel bar), recently vacated the Federal Circuit's 1998 decision.

[125] Culbert, *supra* note 113; A patent entitled "Medical Network System and Method for Transfer of Information," issued to MEDWEB, INC., is one of the first of several patents granted or pending for the routing, management and display of medical imagery data and display over the Internet. U.S. Pat. No. 6,424,996 (issued July 23, 2002). Patents of that type may be subject to more exacting scrutiny by a reviewing court. *Id.*

IV. THE CONTRACT LAW LANDSCAPE

A. Software Programs and Contract Law

Article 2 of the Uniform Commercial Code (UCC), the primary body of commercial contract law in the United States, has long characterized commercial contracts on the basis of the delivery of "goods" or "services." Transactions involving the sale of goods and services are to be characterized using the "dominant purpose" test. If the dominant purpose of the transaction is determined to be the supply of a good, Article 2 governs the transaction. If the dominant purpose of the transaction is determined to be the supply of a service, the transaction is governed by rules of general contract law. The UCC does not provide clear guidance when the contracted for activity calls for the generation, capture, comparison analysis and transmission of information by medical devices.[126]

American courts have begun taking the position that computer software transactions should be construed in keeping with the principles governing the sale of goods outlined in Article 2.[127] Article 2 provides for the imposition of an implied contractual term or warranty with respect to the merchantability of goods. American courts have implied the warranty of merchantability to software transactions.[128] Goods sold for a particular purpose are also subject to the imposition of more stringent contractual terms than those for mass-marketed goods.[129] Article 2 provides an implied warranty of fitness for a particular purpose.[130]

B. Medical Software Contract-Based Performance Duty

American courts have been reluctant to imply terms to contracts that call for the provision of "services." The supplier of a service has traditionally been placed under a contractual duty to carry out the contracted-for services with reasonable care and skill. The *Restatement (Second) of Torts* defines a supplier as "one who undertakes to render services in the practice of a profession or trade [and] is required to exercise

---

[126] *See generally* Noriko Kawawa, *Contractual Liability for Defects in Information in Electronic Form*, 8 BALT. INTELL. PROP. L.J. 69 (1999-2000) (analyzing the law of contracts, torts, and the Uniform Computer Information Transactions Act).

[127] Neilson Bus. Equip. Ctr. Inc. v. Monteleone, 524 A.2d 1172 (Del. 1987).

[128] U.C.C. § 2-314 (1998). The tests for determining merchantability include whether the goods are fit for the ordinary purposes for which such goods are used; whether the goods are adequately labeled as the agreement may require; and whether the goods conform to the promises or affirmations of fact made on the container or label. *Id.*; *see also Neilson*, 524 A.2d at 1172-76 (applying implied warranty of merchantability to computer system).

[129] U.C.C. § 2-314 (1998).

[130] U.C.C. § 2-315 (1998). The implied warranty of fitness for a particular purpose can be attached if the seller at the time of contracting has reason to know any particular purpose for which the goods are required, and the buyer is relying on the seller's skill or judgment to select or furnish suitable goods. *Id.*

the skill and knowledge normally possessed by members of that profession or trade."[131]

Where a professional or trade standard can be proven to exist, the courts may impose a duty of performance at a level commensurate with that standard.[132] The performance of services provided by American medical and legal professionals are subject to the higher standard.[133]

The new FDA and the proposed HHS regulatory frameworks that govern the life-cycle architecture, programming, distribution, and maintenance of medical device software establish a minimum level of skill and competence that must be observed by those who supply medical device software for use in the American health care market. While it is within the capacity of parties to a medical device software contract to attempt to disclaim implied warranties of merchantability or fitness for a particular purpose,[134] contractual terms attempting to disclaim the performance of medical software technology contracts in accordance with either the existing FDA or the proposed HHS regulatory software standards are contrary to public policy and unenforceable.[135]

C. Software Programs and the Proposed Adoption of The Uniform Computer Information Transactions Act

A movement is underway to create the Uniform Computer Information Transactions Act (UCITA), a new body of law that will supply rules governing the licensing of computer software and "computer information transactions."[136] In keeping with its scope, complexity and importance, UCITA has been the subject of great controversy.[137] So far, only two states, Maryland and Virginia, have enacted

---

[131] RESTATEMENT (SECOND) OF TORTS § 552(1) (1976).

[132] 9 S. WILLISTON, A TREATISE ON THE LAW OF CONTRACTS, § 1012 C (3d ed. 1967 & Supp. 1987).

[133] *Id.*

[134] To attempt to disclaim an implied warranty, the disclaimer must conform to the requirements of U.C.C. § 2-316 as interpreted by the courts. In addition to being "conspicuous" and "in writing," attempted disclaimers must survive judicial interpretation of the effects of integration clauses or the doctrine of unconscionability.

[135] U.C.I.T.A., § 406(c) (1999). UCITA allows disclaimer of implied warranties unless the disclaimer would be manifestly unreasonable, pre-empted by federal law, or in violation of a fundamental public policy. *Id.*

[136] *See Draft for Approval of Uniform Computer and Information Transactions Act, available at* http://www.law.upenn.edu/bll/ulc/ucita/citam99.htm (last visited April 15, 2003); *see also UCITA Developments,* National Conference of Commissioners on Uniform State Laws, http://www.nccusl.org/nccusl/ucita/UCITA_Standby_Comm.htm (last visited April 15, 2003).

[137] *See generally UCITA Developments*, National Conference of Commissioners on Uniform State Laws, *at* http://www.nccusl.org; Letters, Statements, Testimony, Resources, *Article 2B of the Uniform Commercial Code*, Uniform Computer Information Transactions Act, Association of Research Libraries, Washington, DC *at* http://www.arl.org/info/letters/index.html; *American Bar Association Working Group Report, Uniform Computer Information Transactions Act ("UCITA"), at* http://www.nccusl.org/nccusl/ucita/UCITA_Standby_Comm.htm (last visited April 15, 2003).

versions of UCITA into law. A nationwide lobbying effort is underway to convince additional state legislatures to enact UCITA.[138]

A recent American Bar Association Working Group Report harshly criticizes UCITA and recommends that it be completely redrafted.[139] Proponents of UCITA oppose redrafting and have offered a number of amendments to UCITA to satisfy objections raised by the Working Group Report.[140]

1. Software Integrated with or Embedded into Goods

Of particular interest here, the ABA Working Group Report criticized the approach UCITA used to resolve issues involving "computer software that is integrated into goods," asserting instead that:

> It is important for users of UCITA to know whether UCITA applies or does not apply to a particular transaction. One of the most difficult and challenging questions raised by UCITA is the extent to which UCITA should apply to software that is integrated into goods. . . .
>
> UCITA addresses this issue by asking two questions: (1) [W]hether the goods are a "computer" (which is defined as an electronic device that accepts information in digital or similar form and manipulates

---

[138] *See Next Few Months the NCCUSL Will Prepare to Take Article 2, UCITA Changes on the Road*, Computer Technology Law Report, Vol. 3, No. 17 (Sept. 6, 2002); *NCCUSL Adopts All Proposed Amendments to UCITA with Some Adjustments to Text*, Computer Technology Law Report, Vol. 3, No.16 (Aug. 6, 2002); *UCITA Drafters Will Entertain Proposals to Make Licensing Law Consumer-Friendly*, Computer Technology Law Report, Vol. 2, No. 22 (Nov. 16, 2001).

[139] As its primary criticism, the ABA Working Group stated:

> [UCITA] as presently drafted, is extremely difficult to understand. [UCITA] is a very complex statute that is daunting for even knowledgeable lawyers to understand and apply. . . . [M]any of the "black letter" rules come across as convoluted and at times, inscrutable. Time and again, when the Working Group attempted to consider the substantive merits of a UCITA concept or provision, the Group had to parse through the language word by word and clause by clause, only to realize, in the end, that the individual members of the Group could not agree on what the particular section said or meant.
>
> Accordingly, the Working Group is concerned that UCITA, as presently drafted, would not achieve the principal objective that a uniform law is expected to achieve, namely, the establishment of a high level of clarity and certainty in a particular area of the law.
>
> To the contrary, the Working Group is concerned that if UCITA, in its present form, goes forward, there would be considerable controversy and litigation over what its various "rules" really mean. . . . [T]he Working Group believes that UCITA should be redrafted to make it easier to understand and use.

American Bar Association Working Group Report, supra note 137, http://www.nccusl.org/nccusl/ucita/UCITA_Standby_Comm.htm.

[140] *Id.* at 9; *see also U.C.I.T.A. 2002 Revisions: Memo and Chart, available at* http://www.nccusl.org/nccusl/ucita/UCITA_082602_MEMO_and_CHART.pdf (last visited Aug. 23, 2002).

it for a result based on a sequence of instructions") or a "computer peripheral" (which term is not defined), and (2) whether access to or use of the software contained in and sold or leased as part of the goods is "ordinarily a material purpose of transactions in goods of the type sold of leased. . . ."

If either the "computer or computer peripheral" test or the "material purpose" test is met, then UCITA applies to the software, and other law, presumably UCC Article 2 (sales of goods) or 2A (leases of goods), applies to the goods. If, on the other hand, either test is not met, the transaction is not governed at all by UCITA, but is instead governed by other law, presumably once again, Article 2 or 2A. . . .

Members of the Working Group felt that this approach created uncertainties and was difficult to apply. The word "computer" is so broadly defined that any goods containing a computer chip might be construed to be a "computer," raising the possibility that all transactions for consumer electronic devices and most transactions for commercial equipment would fall within the scope of UCITA. . . .

Although the Comments to UCITA attempt to explain how the "material purpose" test should be applied to particular transactions, the Working Group is not confident that the Comments are consistent with the text in their conclusions. . . ."

The Working Group recognizes that there may be no bright line to decide when goods with integrated software should be governed, even in part, by UCITA and that any formulation of a resolution will not be perfect. . . .

However, it is the view of the Working Group that the line drawn by UCITA could be better formulated to meet the normal and reasonable expectations of the parties. . . .

[A] better formulation would minimize, for transactions involving the sale or lease of goods with integrated software, the possibility of two different bodies of law -- UCITA and typically Article 2 or 2A -- applying to a sale or lease transaction of a single product. Application of dual legal rules for a single transaction would be especially problematic, given, among other things, the different contract formation provisions and third party rights afforded by each set of rules. . . .

The Working Group believes that a better approach, more consistent with buyer or lessee expectations, would be a formulations based on how the goods are marketed. When software is embedded in and marketed as an integral part of goods, many, if not most, people would consider software to be part of the goods. UCITA therefore

> should not apply to the sale or lease of the goods (containing integrated software). Rather, the sale or lease of (goods containing integrated software) should be governed by Article 2 or 2A. . . .
>
> It would necessarily follow under this formulation that software could still be marketed with goods, so that UCITA would apply to the software but other law would apply to the goods. For example, software loaded onto a general-purpose computer and licensed with the computer would be such a mixed transaction, with UCITA applying to the license for the software and other law applying to the sale of the computer. . . .
>
> Similarly, the license of software loaded onto an appliance but intended to be used with the appliance, the software license would be governed by UCITA while the transaction involving the acquisition of the appliance would be governed by other law. In most cases involving the sale or lease of the goods themselves, in contrast to the license of the software, the other law would be UCC article 2 or 2A, which would apply to the transactions in the goods themselves.[141]

In response, the proponents of UCITA, the National Conference of Commissioners on Uniform State Laws (NCCUSL), reiterated the rationale they used to draft the provision:

> Action: The drafting committee had tried many suggestions, including (the approach suggested by the Working Group), before it settled on the approach in UCITA. . . .
>
> [T]he Committee believes that the current approach best offers guidance to courts and parties for deciding what law should apply. The definition of goods in amended Article 2 of the UCC, recently approved by NCCUSL, excludes "information." The Preliminary Comments to amended Article 2 and the Official Comments to UCITA state that chips (software) embedded in goods in most cases will be governed by UCC Article 2. However, as the working group acknowledges, there is no bright line and in some cases the court will have to determine whether a particular transaction is an information transaction subject to the common law or UCITA, or a goods transaction subject to UCC Article 2.[142]

---

[141] *American Bar Association Working Group Report, supra* note 137, at http://www.nccusl.org/nccusl/ucita/UCITA_Standby_Comm.htm.

[142] *U.C.I.T.A. Developments*, National Conference of Commissioners on Uniform State Laws, U.C.I.T.A. 2002 Revisions: Memo and Chart, Section I. Scope (Aug. 23, 2002).

For now, lawyers are left with a host of unresolved questions regarding the law governing transactions involving "computer software integrated into or imbedded in goods." Will the amended version of UCITA meet with a favorable response from the legislatures of the various states? If the states choose to enact new law will the states accept the position suggested by the proponents of UCITA, the position suggested by the ABA Working Group, or will they devise others? How will the state courts interpret and apply new laws involving "computer software integrated or imbedded into goods?" How should medical software businesses structure their relationships? Further development of the law is sure to follow.

2. Preview of Suggested New UCITA Warranty Law

As some portion of the UCITA warranty framework may become accepted national law, a sampling of the UCITA warranty provisions is appropriate here. Mindful of the criticism of the ABA Working Group about the complexity of UCITA as currently drafted, the reader is urged to examine the cited UCITA provisions and Reporter's Notes to form a professional opinion whether the UCITA warranty provisions should serve as the basis for new national law.

UCITA, Part 4, suggests a new body of warranties be made applicable to transactions governed by UCITA, including: Warranty and Obligations of Quiet Enjoyment, Express Warranty, Implied Warranty of Merchantability of Computer Program, Implied Warranty of Informational Content, and Implied Warranty of System Integration.[143]

The Warranty and Obligations of Quiet Enjoyment provisions hold that licensors in transactions subject to the law will warrant that "no person holds a claim to or interest in the information which arose from an act or omission of the licensor, other than a claim by way of infringement or misappropriation, which will interfere with the licensee's enjoyment of its interest."[144] Licensors of patent rights will warrant that licensed patent rights are valid and exclusive to the extent that exclusivity and validity are recognized. Merchant licensors will warrant that the "information" is delivered free of the rightful claim of any third party way of infringement. Merchant licensors may "quitclaim" informational rights without warranty as to infringement or misappropriation.[145]

The Express Warranty provisions provide for the creation of a warranty of an "affirmation of fact or promise made by the licensor to the licensee . . . which relates to the information and becomes part of the basis of the bargain."[146] An express warranty will not be created for "an affirmation or prediction merely of the value of the information or informational rights," a "display or description of a portion of the information to illustrate aesthetics, market appeal, or the like, of informational

---

[143] U.C.I.T.A. § 401 (1999).

[144] U.C.I.T.A. § 401(b) (1999).

[145] *See generally* U.C.I.T.A. § 401, *Warranty and Obligations Concerning Quiet Enjoyment and Non-Infringement & Rptr's Notes* (2003).

[146] U.C.I.T.A. § 402 (1999).

content," or "a state purporting to be merely the licensor's opinion or commendation of the information or informational rights."[147]

The Implied Warranty of Merchantability of Computer Program provisions provide for the creation of an implied warranty of a merchant licensor that, unless otherwise disclaimed or modified, the computer program will be reasonably fit for the ordinary purposes for which it is distributed, that the program will be adequately packaged and labeled, that the program will conform to the promises or affirmations of fact made on the container or label, and that the warranty may arise form course of dealing or usage of trade.[148]

The Implied Warranty of Informational Content provisions provide that unless otherwise disclaimed or modified, a merchant in a special relationship of reliance with a licensee, who collects, compiles, processes, provides, or transmits informational content, will warrant to the licensee that there is no inaccuracy in the informational content caused by the merchant's failure to perform with reasonable care.[149] The special element of reliance will arise from the relationship, a relationship characterized by the provider's knowledge that the particular licensee plans to rely on data in its own business and expects the provider to tailor the information to its needs.[150]

The Implied Warranty of System Integration provisions provide that, unless otherwise disclaimed or modified, should a licensor have reason to know any particular purpose for which the information is required, and should he have reason to know that the licensee is relying on the licensor's skill or judgment to select, develop, or furnish suitable information, the information will not fail to achieve the licensee's particular purpose as a result of the licensor's lack of reasonable effort.[151] Additionally, the provisions create a new warranty meant to assure a licensee that selected components will function as a system.[152]

No matter what form the proposed new UCITA warranty provisions eventually assume, counsel should always premise opinions regarding the enforceability of medical device software warranty provisions in terms of the duty of the court to render Justice. In that regard, Professor Peter Alces has persuasively argued that software technology has yet to reach the level of context-based, relational maturation such that the courts will likely resolve software disputes use "standard" warranty provisions supplied by scholars.[153] To the contrary, Professor Alces cogently reminds

---

[147] *Id.* § 402.

[148] *Id.* § 403.

[149] U.C.I.T.A. § 404 (1999).

[150] *Id.*

[151] U.C.I.T.A. § 405 (1999).

[152] *Id.*

[153] *See* Peter Alces, *W(h)ither Warranty: The B(l)oom of Products Liability Theory in Cases of Deficient Software Design*, 87 CAL. L. REV. 269 (1999). Courts seeking to do justice will likely resort to the use of strict products liability law in the event that risk shifting warranty provisions fail to strike the appropriate, context based, experientially oriented balance between the rights of producers of software products and the rights of consumers of software product technology who are harmed by the use of defective software. *Id.*

us that the failure of warranty law to render Justice in medical software disputes may open the door to the resolution of those disputes using the law of torts.[154]

V. THE TORT LAW LANDSCAPE

The following excerpts, which appear in the FDA's online "Manufacturer and User Facility Device Experience Database" (MAUDE), illustrate how the use of medical device software can cause patient injury or death.[155]

Software Programming:

> Adverse Event or Product Problem Description:
> Type of Device: Computed Tomography
> Manufacturer: Siemens Medical Systems, Inc.
> Date FDA Received: 12/22/2000
> When the eval/magnify function is used in connection with over eval functions, the result may be an incorrect display of the magnified image.[156]
>
> Adverse Event of Product Problem Description:
> Type of Device: Gama Camera
> Manufacturer: Siemens Medical Systems Inc.
> Date FDA Received: 4/20/2001
> A device malfunction was identified. Under specific conditions software will result in incorrect orientation of acquired patient data in "Spect" mode. This occurs when switching from "Coincidence" mode to "Spect" mode on the Ecam via the patient-positioning monitor, while at the same time there is an acquisition workflow running. The incorrect orientation may cause the displayed image to be reversed in either "left to right" or "top to bottom" directions. It may not be immediately clear to the operator that the image has been reversed. A potential for misdiagnosis exists at that point.[157]

Software Labeling:

> Adverse Event or Product Problem Description:
> Type of Device: Radiation Therapy Planning Equipment
> Manufacturer: ADAC Laboratories
> Date FDA Received: 8/18/1999

---

[154] *Id.*

[155] MAUDE Data Base Record, Food & Drug Administration - Center for Devices and Radiological Health (Emphasis supplied), *available at* http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Search.cfm (last visited Apr. 15, 2003).

[156] *Id.*

[157] *Id.*

> The customer reports that while planning on a Siemens Primus machine the treatment plan printout displays incorrect jaw labels. The Siemens terminology used in jaw orientation specification differs from the Pinnacle software jaw orientation terminology. The treatment plan printout displays the Y jaws labeled as "width" and the X jaws labeled as "length," although Y is in the patient SUP-INF direction and X is the patient Left-Right direction. Confusion over the incorrect jaw labels could lead to problems with the patient being set up incorrectly and/or being treated with the incorrect shape field.[158]
>
> Adverse Event or Product Problem Description:
> Type of Device: Medical Fluoroscopic Mobile C-Arm Software
> Manufacturer: General Electric OEC Medical Systems
> Date FDA Received: 9/8/2000
> The calibration of the automatic brightness control, which regulates the radiation output of the machine was set to excessive values for the "high level pulsed fluoroscopy" mode of operations. OEC claims that their service software does not provide for either means to adjust the radiation dose rate, nor the option to turn off the "high level pulsed fluoro" mode of operation. The purpose of this mode of operation is to acquire a series of individual data images for a predefined time period - "run time" - the individual image files are stored on the imaging computer hard-drive for later retrieval. The images acquired during the serial "run" can undergo automatic or operator controlled digital processing such as image subtraction, edge enhancement, contrast scale modification and serial playback . . . . Instead of labeling the mode of operation "digital acquisition" or "digital cine" (OEC) call it "high level pulsed flouro." This is clearly a misnomer as the mode is not intended for live fluoroscopic viewing.[159]

Software Misuse:

> Adverse Event of Product Problem Description:
> Type of Device: Computer
> Manufacturer: Radionics, a division of Tyco HealthCare
> Date FDA Received: 1/04/99
> This report is based on info supplied by others. Around the date of April 10, 1998, a surgeon used the wrong software package with companies SCS1. The result was that the wrong coordinates were calculated, and consequently, the hole was drilled in the wrong area of the patient's head. Company sales representative from this area was asked to gather info about this event on three separate occasions. These attempts were made on April 21, 1998, May 1, 1998, and May 7, 1998 with no response.

---

[158] *Id.*
[159] *Id.*

> Company is currently in the process of evaluating the labeling of this product to possibly additional warnings to the software packages.[160]
>
> Adverse Event or Product Problem Description:
> Type of Device: Computerized Treatment Planning System
> Manufacturer: Multidate Systems International Corp.
> Date FDA Received: 6/16/2001
> In public documents released by the International Atomic Energy Agency (IAEA) and the US Nuclear Regulatory Commission (US NRC), Multidate has become aware of a radiological emergency in Panama . . . . The emergency involved a radiotherapy unit using a Cobalt-60 teletherapy machine and a computerized treatment planning system for calculating radiation doses to be delivered to the patient. [A Panamanian] Health Minster said health officials changed their procedures in administering the radiation treatment in order to get better results and ended up giving the patients between 20% to 100% more radiation than they should have. As reported, the incident involved 28 patients who were treated at the [National Oncology Institute of Panama] from 2000 through 2001 for colon, prostrate and cervical cancer. Eight of the patients are reported to have died, and five of the deaths have been attributed to the excess radiation received during the treatments . . . . The practice at the facility was changed to enter data in such a way as to appear to the treatment system to exceed its limitation on shielding blocks, even though the user manual for the treatment planning system not only clearly specifies the limit, but also recommends that the results be verified by measurement before using.[161]

A. Negligence Law

Attorney-software engineer Cem Kaner provides useful baseline observations about the applicability of negligence law to computer software. Kaner explains, "[T]he essence of quality-related litigation is a customer seeking to transfer losses caused by a defective product back to the company that made the defect or sold it."[162] Kaner surmises that the quality costs associated with software products include:

> [e]xternal failure, technical support calls, preparation of support books, investigation of customer complaints, refunds and recalls, coding/testing of interim bug fix releases, shipping of updated product, added expense of supporting multiple versions of the product in the field, PR work to soften drafts of harsh reviews, lost sales, lost customer goodwill, discounts to resellers to encourage

---

[160] *Id.*

[161] *Id.*

[162] Cem Kaner, *The Law of Software Quality, available at* http://www.kaner.com/pdfs/slides/amslaw.pdf (last visited Apr.15, 2003).

> them to keep selling the product, warranty costs, liability costs, government investigations, penalties, and all other costs imposed by law. [163]

A customer who buys a defective product absorbs costs such as "wasted time, lost data, failure during tasks that can only be done once, cost of replacing product, reconfiguring the system, cost of recovery software, cost of tech support, and injury/death."[164] Kaner adds that "[r]easonable consumers have reason to sue if [the manufacturer's/seller's] products' failures cost them more than their cost and aggravation from litigation."[165]

1. Software Programs, the Law of General and Professional Negligence, and the Supply of Medical Device Software

A showing of the elements of a negligence action are proof that defendant was subject to a legal duty to exercise reasonable care, that defendant breached the duty of care, that defendant's breach of duty was the factual and legal cause of plaintiff's injury, and that plaintiff suffered actual loss or damage as a result.[166] Defendant may be the subject of a higher duty of care if the defendant holds himself out as possessing special skills and training.[167]

In a series of professional publications and presentations, Cem Kaner has convincingly documented the applicability of negligence law to computer software.[168] Software programmers are under a duty to create products that do not create an unreasonable risk of injury or property damage, and to provide services of a quality that would be provided by a reasonable member of the software programming industry.[169] Mr. Kaner has identified several causes of action for software negligence, including negligent pre-sale misrepresentation, negligent programming, negligent software testing, negligent software quality control planning, professional negligence, and negligent post-sale misrepresentation.[170]

Today's international technology economy depends on the supply of human creativity from the following three sources: designers and developers who design, manufacture, and distribute technology products; designers and developers who license their designs to others to refine, manufacture, and distribute; and independent designers who apply their professional skills to create technological designs for products that satisfy market needs.[171]

---

[163] *Id.* at 34.

[164] *Id.* at 28.

[165] *Id.* at 30.

[166] RESTATEMENT (SECOND) OF TORTS § 281 (1979).

[167] Kaner, *supra* note 162, at 22.

[168] *See e.g.,* Cem Kaner, *The New Legal Regime, Bad Software and a Place for Certification, available at* http://www.kaner.com/pdfs/slides/lawcert.pdf (last visited April 15, 2003).

[169] *See* Kaner, *supra* note 162, at 194-95.

[170] *Id.* at 193-252.

[171] *See generally* Melissa Evans Buss, *Products Liability and Intellectual Property Licensors,* 27 WM. MITCHELL L. REV. 299 (2000).

As applied to the three sources of technology design, PreMarket Submissions, Off the Shelf Software, and Software Validation combine to create a composite standard similar to those used to regulate the practice of the learned professions. Just as a trial lawyer must know the rules of evidence and appellate procedure, a medical device software engineer must know and practice the rules of software risk analysis and statement coverage. Just as an orthopedic surgeon must know the anatomy of the human skeletal system and current surgical practice, a medical software engineer must know and practice the rules of software risk and statement coverage.

As such, injured persons, as individuals or as members of a class, can now be expected to use the courts to demand that medical device software venturers, medical device manufacturers and distributors, and medical software intellectual property holders lawfully discharge their duty to architect, develop, document, distribute and maintain safe and efficacious medical software.[172]

The time is at hand when the courts will demand that the general practice of software engineering conform its conduct to the level of conduct practiced by the medical software industry; this particularly presents a special concern to the general commercial software industry. The law in that regard is clear. The courts impose a legal duty of care in the absence of reasonable conduct on the part of industry; liability for breach of a duty of care will be imposed where the burden of prevention is less than the probability of an accident and the gravity of the resulting harm.[173]

The social demand for secure, private, safe and effective software ensures that the new federal regulatory medical software standard will inexorably migrate to the general commercial software industry. The general commercial software industry will soon be subject to much broader liability then it is now accustomed to. It is only a matter of time.

2. Software Programs and the Law of Products Liability

For the past forty years, American medical device law has been guided by Section 402A of the *Restatement (Second) of Torts*.[174] The underlying premise of the

---

[172] *Contra* Jonathan K. Gable, *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, 5 QUINNIPIAC HEALTH L.J. 127, 143 (2001). "The likelihood that a simple negligence claim would succeed is very slim given a consistent refusal by the courts to hold software providers to the higher duty of care." *Id.*; W. Robert Collins, *How Good is Enough? An Ethical Analysis of Software Construction and Use*, Communications of the Association for Computing Machinery, (Jan. 1994); Cem Kaner, *The Law of Software Quality*, 248 (1999).

[173] United States v. Carroll Towing, 132 F.2d 170 (2d Cir. 1947) (Hand, J.). Courts will impose liability for breach of a duty of care where the burden of prevention is less than the probability of an accident times the gravity of the resulting harm. *Id.* at 173; The T. J. Hooper, 60 F.2d 737 (2d Cir. 1932) (Hand, J.). "There are, no doubt, cases where courts seem to make the general practice of the calling the standard of proper diligence. *Hooper*, 60 F.2d at 740. "Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices." *Id.* "[T]here are precautions so imperative that even their universal disregard will not excuse their omission." *Id.*

[174] RESTATEMENT (SECOND) OF TORTS § 402A (1965); *see* Michael J. Wagner & Laura L. Peterson, *The New Restatement (Third) of Torts - Shelter from the Product Liability Storm for*

Restatement, as adopted by the vast majority of American courts and state legislatures, is that the manufacturer or seller of a defective product that is unreasonably dangerous to the user or consumer is liable for physical harm caused by the product.[175]

The *Restatement (Second)* devoted almost no coverage to the treatment of the liability for prescription drugs and medical devices. The only relevant insights appear in the infamous "comment k":

> *Unavoidably unsafe products.* There are some products, which, in the present state of human knowledge, are quite incapable of being made safe for their intended and ordinary use. These are especially common in the field of drugs. An outstanding example is the vaccine for the Pasteur treatment of rabies, which not uncommonly leads to very serious and damaging consequences when it is injected. Since the disease invariably leads to a dreadful death, both the marketing and use of the vaccine are fully justified, notwithstanding the unavoidable high degree of risk, which they involve. Such a product, properly prepared and accompanied by proper directions and warning, is not defective nor is it unreasonably dangerous.[176]

"Comment k" prompted the American courts and state legislatures to adopt inconsistent and contradictory products liability laws.[177] Among other things, "comment k" has prompted the courts to consider whether the court or the jury should weigh risks and benefits to determine whether a product falls within the reach of "comment k" coverage.[178] Citing "comment k" for guidance, leading state courts have reached differing positions on identical issues. The California Supreme Court recently announced a rule imposing strict liability on manufacturers for the failure to disclose known or knowable risks.[179] In contrast, the Washington Supreme Court held that manufacturers could be held liable only for their negligent failure to disclose known or knowable risks.[180]

It is unlikely that a reviewing court would consider "comment k" to constitute useful guidance for the resolution of a medical device software tort action. "Comment k" was included in *Restatement (Second)* 402(A) as an exception to the rule of strict liability for products, like the rabies vaccine, that are by necessity of design or intended use, "unavoidably unsafe" yet highly beneficial to society. The new FDA regulations for the architecture, development, and maintenance of medical software would almost surely prohibit a grant of conditional FDA approval for the marketing

---

Pharmaceutical Companies and Medical Device Manufacturers?, 53 FOOD DRUG & COSM. L.J. 225, 226 (1998).

[175] *See generally* Wagner & Peterson, *supra* note 174, at 226-27.

[176] RESTATEMENT (SECOND) OF TORTS, § 402A cmt. k (1965).

[177] *See* Wagner & Peterson, *supra* note 174, at 231 (ongoing debate between courts, law review commentators, and even the comment's reporters exists due to the ambiguous language contained within "comment k").

[178] *Id.*

[179] Carlin v. Superior Court, 920 P.2d 1347 (Cal. 1996).

[180] Young v. Key Pharms., Inc., 922 P.2d 59 (Wash. 1996).

of medical software programs that by design were known to be unsafe and could not be rendered safe within the FDA guidance structure.

Technology designers have, in fact, been named as defendants in products liability lawsuits.[181] The case law generally holds that the technology designer who remains involved in the manufacture and distribution of a defective product, and the independent technology designer whose design is later used to manufacture and distribute the defective product, can be held liable in products liability to third parties whose injuries are caused by the designer's negligence.[182] The technology designer who does not "substantially participate" in the design of the marketed product is excused from liability. "Substantial participation" is determined on the particular facts of the case.[183]

Computer software standards organizations, commentators and attorneys have suggested a variety of definitions to be used to characterize software "defects" that would render a software program a "defective product" within the meaning of Section 402(A):

> Defect: A product anomaly. Examples include such things as (1) omissions and imperfections found during early life cycle phases and (2) faults contained in software sufficiently mature for test or operation.[184]
>
> Anomaly: Any condition that deviates from expectations based on requirements specifications, design documents, user documents, standards, or from someone's perceptions or experiences. Anomalies may be found during, but not limited to, the review, test, analysis, compilation, or use of software products or applicable documentation.[185]

Software defects can be divided into four broad categories: (1) requirements defects, (2) design defects, (3) code defects, and (4) documentation defects.[186] There is a group of software nonconformities that represent serious threats to the welfare of users and bystanders. These nonconformities are called defects, and they not only can cause injury but may also result in the manufacturers, designers, or sellers being sued under the product liability laws. There is also a class of defects called design defects, which can be responsible for customer dissatisfaction, loss, injury or death.[187]

---

[181] *See* Buss, *supra* note 171, at 311-14.

[182] *Id.* at 311.

[183] *Id.*

[184] ANSI/IEEE STANDARD 982.1, IEEE STANDARD DICTIONARY OF MEASURES TO PRODUCE RELIABLE SOFTWARE, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, p. 13 (1988).

[185] *Id.* at 3.

[186] *See* WILLIAM H. ROETZHEIM, DEVELOPING SOFTWARE TO GOVERNMENT STANDARDS 6-7 (Prentice-Hall 1991).

[187] General Motors v. Johnston, 592 So.2d 1054 (Ala. 1992). Programmable Read Only Memory chip containing modified software controlling the fuel injector in Chevrolet truck may have caused "rolling, hunting or surging idles" that were cause of plaintiff's injuries. *Id.*

The issue becomes more important in the context of the clear trend of international commerce to integrate or to imbed software into goods and human beings.[188] Moreover, successive applications, refinements and enhancements of technologies often render indistinguishable the original labels used to distinguish the technologies as "computers," "chips," "hardware," or "software."[189] The same holds true for the types and forms of intellectual properties that are integrated or imbedded into software.[190]

Section 6 of the new *Restatement (Third) of Torts: Products Liability*, is being considered as a source of guidance for the courts.[191] The *Restatement (Third)* includes special provisions applicable to prescription drugs and medical devices.[192] Section 6(c) of the *Restatement (Third)* states:

> A prescription drug or medical device is not reasonably safe due to defective design if the foreseeable risks of harm posed by the drug or medical device are sufficiently great in relation to its foreseeable therapeutic benefits that reasonable health care providers, knowing of such foreseeable risks and therapeutic benefits, would not prescribe the drug or medical device for any class of patients.[193]

The suggested *Restatement (Third)* standards present a series of startling changes to the generally accepted legal standards used to evaluate drug and device liability in products liability actions. The suggested standard would limit liability to only those medical devices that provide *no* benefits to *any* identifiable class of patients.[194] The suggested standard would shift the burden of knowledge concerning the performance of medical device products from manufacturers to the prescribing physicians.[195] In some states, the suggested standards would shift the burden of proof that a medical device is not reasonably safe to the plaintiff.[196] As such, the suggested standards are open to serious challenges.

---

[188] *See generally* Steven Kotler, *Vision Quest: A Half-Century of Artificial Sight Research as Succeeded. And Now This Blind Man Can See,* WIRED, (Sept. 2002) (asking what liability for technology designers and manufacturers who mass market new bio-engineered products that are implanted in the human brain).

[189] *See* Cem Kaner & David Pels, Report to the Federal Trade Commission, *In the Matter of High Technology Warranty Project*, FTC File No. P994413 (Sept. 11, 2000).

[190] Buss, *supra* note 171, at 311-14 (providing an analysis of *Alm v. Aluminum Co. of America,* 717 S.W.2d 588 (Tex. 1986), *Mechanical Rubber & Supply Co. v. Caterpillar Tractor Co.*, 399 N.E.2d 722 (Ill. App. Ct. 1980), and *La Rossa v. Scientific Design Co.,* 402 F.2d 937 (3d Cir. 1968)).

[191] *See* Buss, *supra* note 171, at 280.

[192] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY (1998); *see generally* Wagner & Peterson, *supra* note 174, at 228-29; Harvey L. Kaplan, et al., *Third Restatement: New Prescription for Makers of Drugs and Medical Devices: Third Restatement of Torts Draft*, 61 DEF. COUNS. J. 64 (1994).

[193] RESTATEMENT (THIRD) OF TORTS § 6 (1998).

[194] *See* Wagner & Peterson, *supra* note 174, at 233 (citing RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 6, cmt. f, reporters' note).

[195] *Id.* at 234.

[196] *Id.* at 235.

The suggested standards fail to properly distinguish between drugs and devices and make no mention of medical device software. The underlying scientific premise supporting the development of medical software is that human tissue, compounds, and molecules are nearly identical throughout the species. Unlike prescription drugs, medical software devices of the type described here are intended to gather, filter, and analyze data on a consistent, repetitive, scientifically accurate basis. Thus, the ingestion of a pharmaceutical compound should not be legally equated with the use of an electronic algorithm to analyze the depiction of interaction of energy waves with human tissue, compounds and molecules.

The reality of professional medical practice is that with respect to the use of medical software and medical devices using integrated or embedded medical software, a treating physician has no other choice but to rely on manufacturer representations. Physicians cannot be expected to possess the scientific training necessary to comprehend the entirety of the design and manufacture of a medical device software technology. Only the medical software technology designers and manufacturers are positioned to know the capacities and operational tendencies of their equipment.

The suggested standard is squarely at odds with the intent of the FDA regulatory scheme. Manufacturers of medical device products must demonstrate, or "validate" in the case of medical software, that the medical devices they intend to market are safe and efficacious before the FDA will grant conditional approval of devices for market use.

Although the suggested standard supports the use of a "reason based alternative-design approach," the standard does not provide for the application of strict products liability doctrine followed in many American states. In view of the fact that mass torts may result from the use of widely distributed, intensely market-focused, defective medical device software, the "reason based alternative-design approach" may afford defendants a proof advantage that their actions do not warrant. For example, should classes of persons whose "individually identifiable health information" is lost, stolen, scrambled, or corrupted be required to prove the negligence of each of the medical software components involved? I think not.

Further, the suggested standard makes no allowance for the likelihood that injuries arising from the use of medical software may be found to be the result of the interaction of *two or more* faulty software programs. In that instance, general negligence law would allow the injured plaintiff to hale in both of the injury causing software product manufacturer-distributors to prove his injury, and then require the defendant, software product manufacturer-distributors, to prove that their individual negligence was not the cause of the plaintiff's injury.

Finally, the Article 6(c) standard seems to be based on the theory that licensed, practicing medical professionals would prescribe the use of a medical device knowing that the device supplied no medical benefit to any class of identifiable class of patients. The standard seems to embody the principles of quackery, the antithesis of professional medical practice, as the baseline point for the imposition of liability.

Thus, the only rationale that can be offered for the suggested changes is that they were drafted to attempt to insulate drug and device manufacturers from

liability.[197] On balance, with respect to resolution of disputes and the allocation of liability involving harm caused by the use of medical device software, I believe a reviewing court will likely reject the Article 6(c) suggested standards. Thus, business models and operational strategies premised on the supposed grant of limitation of liability offered by Article 6(c) standards are faulty.

Whether the courts will accept *Restatement (Third)* guidance for medical device products in general, and for medical device software in particular, is an open question. The record thus far is mixed. Several states have openly repudiated the *Restatement (Third)*.[198] In view of the utter reliance a patient places on the quality of care he will receive at the hands of his physician, the suggested *Restatement (Third)* guidance for medical devices that integrate or imbed medical device software is incorrect. The standards of our time and the time to come demand far more than the *Restatement (Third)* provides.

B. Tort Law Preemption of FDA Regulation

For some years, it was common practice to assume that federal FDA pre-market approval preempted common law causes of action, thus immunizing FDA-approved medical devices against state common law liability.[199] In that same vein, the *Restatement (Third)* mildly advocates federal preemption of common law causes of action with respect to warnings affixed to drugs and medical devices.[200]

The Supreme Court addressed this issue in *Medtronic v. Lohr*.[201] Justice Stevens rejected Medtronic's position that the Medical Device Amendments Act of 1976 preempted common law claims against manufacturers for damages caused by medical devices. Justice Stevens reasoned that the general common law duties to use due care in manufacturing and to warn users of potential risks posed no threat to federal requirements, and such duties were not the type of requirements that impede the ability of the FDA to enforce specific federal laws and regulations.[202]

---

[197] *Id.* at 242.

[198] Carlin v. Superior Court, 920 P.2d 1347 (Cal. 1996); Wagner & Peterson, *supra* note 174, at 240.

[199] *See generally* Green & Shultz, *supra* note 16, at 2123-28 (analyzing the merits of a FDA pre-emption defense); Lars Noah, *Rewarding Regulatory Compliance: The Pursuit of Symmetry in Products Liability*, 88 GEO. L.J. 2147 (2000); Richard B. Stewart, *Regulatory Compliance Preclusion of Tort Liability: Limiting the Dual-Track System*, 88 GEO. L.J. 2167 (2000); Rachel Tumidolsky, *How* Medtronic v. Lohr *Has Redefined Medical Device Regulation and Litigation*, 65 DEF. COUNS. J. 268, 269-76 (1998).

[200] RESTATEMENT (THIRD) OF TORTS § 6, cmt. b (1998).

> The rules imposing liability on a manufacturer for inadequate warning or defective design of prescription drugs and medical devices assume that the federal regulatory standard has not preempted the imposition of tort liability under state law. Where such preemption is found, liability cannot attach when the manufacturer has complied with the applicable federal standard.

Id.

[201] Medtronic v. Lohr, 518 U.S. 470 (1996).

[202] *Id.* at 501-02; *see also* Tumildosky, *supra* note 199, at 271 (discussing how FDA-imposed requirements preempt state common law duties when the FDA has expressly imposed, by regulation

By way of example, the recent holding of the United States District Court for the District of Virginia in *Woods v. Gliatech, Inc.,*[203] follows the line of cases interpreting the *Medtronic* rule. Defendant Gliatech developed, tested, distributed and marketed ADCON-L, a Class III gel product used to inhibit post-surgical growth of scar tissue. Gliatech failed to notify the FDA that surgeons were reporting adverse medical reactions in surgical patients treated with the gel.[204] Relying on the information submitted by Gliatech, the FDA granted conditional approval for the marketing of ADCON-L.[205] The court ruled that the FDA's conditional pre-market approval of the gel, and the FDA's accompanying findings regarding the gel's safety and effectiveness, did not create a specific federal requirement triggering preemption.[206] The court thus allowed plaintiff to proceed with common law claims of negligence and breach of warranty arising from injuries suffered as a result of the medical use of defendant's gel.[207]

1. Tort Law and the Uniform Computer Information Transactions Act

The new UCITA warranty provisions have the effect of limiting or denying altogether the ability of third parties to recover for a breach of a UCITA warranty. The Reporter's Notes make it clear that the UCITA warranty provisions were drafted so as to minimize the reach of tort law:

> *Third Parties.* This section deals with express warranties made by the licensor to its licensee. It does not deal with the enforceability under contract or tort theory of representations made by remote parties and relied on by an ultimate user of information. Cases in tort dealing with such issues pertaining to information does not generally parallel cases dealing with the manufacture and sale of goods. Information providers have been held liable to third parties in only a few, atypical cases. This Act does not establish, expand or exclude such third party liability.[208]
>
> *Relationship to Tort Law:* Since this section creates a new warranty analogous to the theory of negligent misrepresentation, disclaimer or

---

or order, a specific substantive requirement applicable to a particular medical device and state common law imposes a substantive requirement applicable to the same particular medical device that is different from or in addition to, any requirement applicable to the FDA requirement); 21 C.F.R. § 808 (1996); *see also* Buckman Co. v. Plaintiffs' Legal Committee, 531 U.S. 341, 347-48 (2001) (explaining that state law causes of action based solely on fraudulent misrepresentations made to the FDA to obtain market approval are impliedly preempted).

[203] 218 F. Supp. 2d 802 (W.D. Va. 2002).

[204] *Id.* at 803.

[205] *Id.* at 803-04.

[206] *Id.* at 808.

[207] *Id.*; *see also Surgical Gel: Federal Law Does Not Bar Claims Against Maker of Faulty Gel Product*, PRODUCT LIABILITY DAILY (September. 12, 2002).

[208] U.C.I.T.A., § 402, Reporters' Note § 9 (2001) (Draft).

> non-existence of the implied warranty should have a bearing on existence of the tort claim in the same transaction. In cases of economic loss, a disclaimer of this warranty in most cases forecloses a tort claim based on the same facts. However, this section does not foreclose development of other approaches under tort law. . . . This Act neither precludes nor encourages further exploration of the tort law questions.[209]
>
> *Products Liability Law*: This section does not deal with products liability issues. It neither expands nor restricts tort concepts that might apply for third party risk, leaving development or non-development of any appropriate liability doctrine to common law courts. Indeed, few courts impose third-party tort liability in transactions involving information. The *Restatement (Third)* on Products Liability, recognizing this, notes that informational content is not a product for that law. . . . While there may be a different policy for software embedded in tangible products, this Act does not deal with embedded software. Contract issues regarding such software, such as the computer program that operates the brakes in an automobile sold to a consumer, are within the Uniform Commercial Code.[210]

The purpose of medical device software is to provide accurate and reliable information that can be used to diagnose and treat human illness. The efforts taken by the drafters of UCITA to distance UCITA from the host of issues that arise from transactions in medical information in general, and individually identifiable health information in particular, should be changed to reflect the practical reality unfolding in the American medical profession. The UCITA warranty provisions should be drafted to affirmatively state that liability in tort may exist for negligently drawn, developed, distributed, and maintained medical device software.

2. New Medical Software Torts

The FDA and HHS regulatory frameworks will combine to impose legal duties that regulate the creation, storage, and transmission of digital, individually identifiable health information. Inevitably, patients will be injured by the improper distribution, loss, alteration, or corruption of their personal data.

Injured patients can be expected to capitalize on the legal duties created by the FDA scheme and the proposed HHS regulatory schemes to impose tort liability on medical software designers, businesses that market medical software, businesses that market medical devices that integrate or imbed medical software, and holders of medical software intellectual property rights that cause injury.

---

[209] U.C.I.T.A., § 6 (2001).

[210] U.C.I.T.A. § 409, Reporters' Note § 3 (2001).

a. Privacy Tort: The Unlawful Use of Individually Identifiable Health Information

The unlawful use of "individual health information" is a federal felony.[211] The "knowing misuse" of "individually identifiable health information" carries a fine of not more than $100,000 and imprisonment of not more than five years or both. The "misuse" of "individually identifiable health information" with intent to sell, transfer, or use of individually identifiable health information for commercial advantage, personal gain, or malicious harm carries a fine of not more than $250,000 and imprisonment of not more than 10 years or both.[212]

Pursuant to the well-established doctrine of negligence *per se*, a precise standard of care in a tort action may be established by proof of the applicability to the case of a statute providing for criminal penalties. When such proof is shown, the specific statutory duty imposed by the criminal statute replaces the general common law duty of care.

Proof of negligence *per se* requires the plaintiff to prove that he is in the class of persons protected by the criminal statute, that the statute was intended to prevent the type of harm that he suffered, and that the statute clearly proscribes the actions of the defendant. Breach of the duty imposed by a criminal statute is *prima facie* evidence of negligence to be considered by the trier of fact.

This new tort is a cousin to the existing common law tort of public disclosure of private facts. The rationale for the common law tort rests in the wrongful publication or public disclosure by the defendant of private information about the plaintiff that a reasonable person of ordinary sensibilities would object to having been made public.

b. Security Tort: The Negligent Disclosure, Alternation or Loss of Individually Identifiable Health Information

The excerpts that follow below appear as portions of the "Proposed Rule for Security and Electronic Signature Standards" published by the Health Care Financing Administration of the HHS.[213] Final rules are expected near term. The structure of the Proposed Rule strongly suggests that HHS will follow the regulatory example set by FDA. Thus, the final HHS regulations will likely establish a broad composite standard that can be used as a statutory standard of care regulating the electronic exchange of "individually identifiable health information":[214]

---

[211] Security and Electronic Signature Standards, 45 C.F.R. § 142 (2002).

[212] *Id.*

[213] *See id.*

[214] 45 C.F.R. § 142 (2002). Portions of the proposed rule became effective in October 2002 for health care clearinghouses and health care provider that chooses to transmit any of the transactions in electronic form, and will become effective in October 2003 for small health care plans. *Id. See* U.S. DEP'T OF HEALTH AND HUMAN RESOURCES, *Frequently Asked Questions About Electronic Transaction Standards Adopted Under HIPAA, available at* http://asppe.hhs.gov/adminsimp/faqtx.htm (last visited April 14, 2003); U.S. DEP'T OF HEALTH AND

> There is no recognized single standard that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and technical mechanisms) that must be in place to preserve health information confidentiality and privacy as defined in the law. Therefore we are designating a new, comprehensive standard, which defines the security requirements to be fulfilled. . . .
>
> In fact, there are numerous security guidelines and standards in existence today, focusing on the different techniques available for implementing the various aspects of security. We thoroughly researched the existing guidelines and standards and consulted extensively with the organizations that developed them. . . .
>
> The standard does not address the extent to which a particular entity should implement the specific features. Instead, we would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions each organization would have to make. . . .

The recommendations contained in the National Research Council's 1997 report *For The Record: Protecting Electronic Health Information* support our approach to the development of a security standard. . . . The report concludes that appropriate security practices are highly dependent on individual circumstances, but goes on to suggest that [i]t is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities and risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another. . . . Inherent in this approach is a balance between the need to secure health data against risk and the economic cost of doing so. Health care entities must consider both aspects in devising their security.

The proposed security standard addresses the following policies, practices, and procedures:

Technical Practices and Procedures

1. Individual authentication of users

HUMAN RESOURCES, *What are the major differences between the proposed rule and the final rule?*, *available at* http://asppe.hhs.gov/adminsimp/faqtx.htm (last visited April 14, 2003).

2. Access controls
3. Audit trails
4. Physical security and disaster recovery
5. Protection of remote access points
6. Protection of external electronic communications
7. Software discipline, and
8. System assessment.

Technical Security Services to Guard Data Integrity, Confidentiality and Availability

1. Access Control
2. Audit Control
3. Authorization Control
4. Data Authentication
5. Entity Authentication.[215]

Persons injured by the negligent disclosure, loss, or alteration of personal, individually identifiable health information can be expected to look for recovery from all persons or entities who had access to, or were involved in, the electronic transmission of personal medical information.

In the absence of statutory change, the liability of physicians and their agents for the negligent disclosure, loss, or alteration of digital individually identifiable health information will be determined using the laws of professional negligence. The liability of digital intermediaries for the negligent disclosure, loss, or alteration of personal, individually identifiable health information will be governed by the Digital Millennium Copyright Act.[216] The liability of medical software designers, businesses that market medical software, and medical software intellectual property rights holders will be determined using the FDA and HHS regulatory standards. Under either or both of the FDA or HHS regulatory standards, liability in tort for the negligent disclosure, alternation or loss of individually identifiable health information is here to stay.

VI. COUNSELING THE MEDICAL SOFTWARE VENTURE

The development of a business model for a medical software venture is a very complex, iterative task. The sophistication of the technology, the fact that medical software may be associated with, integrated into, or imbedded into medical devices, and the nature of the various intellectual property rights involved, present an unusually complex planning task requiring the application of sophisticated business

---

[215] 45 C.F.R. § 142 (2003).

[216] 17 U.S.C. § 512 (2002). Sections 512(a) and (c) provide "safe harbor" exemptions for passive carriers and for system storage activities at the direction of the user. *Id.*; *see also* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995); A & M Records, Inc. v. Napster Inc., 54 U.S.P.Q.2d 1746 (N.D. Cal. 2000).

judgment and legal advice. Reasonable prudence requires in-depth thought and considered action.

The business strategy of the medical software venture serves as the base point for analysis. How do the principals of the venture intend to market the medical software? Do they intend to form their own marketing and manufacturing operations for the software and the medical devices that use the software? Do they intend to market the medical software through a cross-licensing agreement with a strategic partner? Do they intend to license the medical software to a major medical device manufacturer? Do they intend to sell the medical software to the highest bidder?

Unlike most new software products in the software industry, medical device software will likely have a lengthy commercial life. It will probably be easier to design products around medical device software than it will be to rewrite the software itself. Medical software ventures will wish to avoid the cost of repetitive encounters with the FDA "validation" process: they will be averse to subjecting their sophisticated, FDA-approved, field-tested code to rapid revision.

The mix of types of intellectual property available for the protection of medical software is especially complex. In view of the fact that medical software can be integrated with or imbedded in other medical devices, careful attention must be paid to the choices of types of property rights sought. The principals of the venture must understand how the complex mix of intellectual property software can be used to attain their business objectives.

Patent and copyright protection can be used to protect different segments of a software program.[217] The copyright symbol may be placed on drawings illustrating a patent application.[218] The General Counsel to the Copyright Office has determined that patent law and copyright law protection may co-exist in computer programs.[219]

Patent and trade secret protection in software programs are typically mutually exclusive.[220] To obtain software patent protection, the applicant must disclose related trade secret data necessary to allow one skilled in the software art to practice the learning that is disclosed in the patent.[221] However, an innovative software subroutine at the heart of the program can be protected by patent while the main body of the program remains a trade secret.[222]

Copyright and trade secret protection may co-exist in a software program.[223] The Code of Federal Regulations contains provisions stating that software being submitted for copyright registration may contain redacted trade secret information if the remainder contains "an appreciable amount of original computer code."[224] Computer programs may simultaneously contain literary works protected by the

---

[217] *See* Judith Szepesi, *Maximizing Protection for Computer Software*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 173, 194-95 (1996).

[218] MANUAL OF PATENT EXAMINING PROCEDURES, § 608.01(v) (1995).

[219] *Contra* Michael Kline, *Requiring an Election of Protection for Patentable/Copyrightable Computer Programs*, 6 COMPUTER/L.J. 607, 638-75 (1986); David A. Einhorn, *Copyright and Patent Protection for Computer Software; Are They Mutually Exclusive?*, 30 IDEA 265, 274-75 (1990).

[220] Szepesi, *supra* note 217, at 195.

[221] White Consol. Indus. v. Vega Servo Control, Inc., 713 F.2d 788 (Fed. Cir. 1983).

[222] *Id.*

[223] Szepesi, *supra* note 217, at 196.

[224] 37 C.F.R. § 202.20(vii)(A)(2) (2002).

federal copyright law, as well as processes and software programs protected under trade secret law.[225] Although copyright law allows "fair use" decompiling of a program to obtain program information that is non-copyrightable,[226] decompiled program language may retain trade secret protection if the code is the subject of a license agreement between the parties that prohibits reverse engineering.[227]

The cost of obtaining and maintaining protection for intellectual property rights in medical device software must be factored into the strategic business model. Patent prosecutions, intellectual property landscape surveys, and validity/non-infringement opinion letters of counsel can easily cost many tens of thousands of dollars. Maintaining a vigorous, effective in-house trade secret program is an expensive necessity.

Medical device software litigation is a certainty. The prosecution or defense of a software patent infringement suit can be expected to cost a minimum of $1,000,000 per party; the prosecution or defense of a copyright or trade secret infringement action can be expected to cost a minimum of $250,000 per party. New forms of intellectual property insurance coverage are being marketed to insure against the costs of intellectual property rights suits brought against technology ventures. Even so, it may become strategically necessary for the venture to fund critical intellectual property rights using the venture's precious cash resources.[228]

VII. PROPOSED GUIDELINES

With all of the above considered, I offer these summary guidelines:

1. A medical software venture must vigilantly strive to understand what intellectual property it has created and owns, as well as what intellectual property it has not created and does not own. All information and data created by the venture is probably the subject of one or more forms of intellectual property law; each of which, should be recognized, protected, and exploited. All information and data that has not

---

[225] Comprehensive Techs. Int'l, Inc. v. Software Artisans, Inc., 3 F.3d 730 (4th Cir. 1993).

[226] Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, n.7 (9th Cir. 1992).

[227] *See generally* Szepsis, *supra* note 217, at 197-203.

[228] *See Chubb Launches New 'Scalable' Errors & Omissions Insurance for High-Tech Industry*, SPEECH TECHNOLOGY MAGAZINE, AMCOMM HOLDINGS (July 23, 2002), *available at* www.speechtechmag.com/pub/industry/971-1.html. Several major insurance companies now offer technology risk insurance. *Id.* American International Companies market the AIG eBusiness Risk Solutions family of policies that insure risks associated with establishing an Internet business, delivering professional services via the Internet, or conducting e-commerce. *Id.* The AIG net Advantage Complete insurance policy provides up to $25,000,000 liability insurance coverage for risks of loss arising from Web Content Liability, Professional Errors and Omissions, Network Security Liability, Cyber Extortion, Network Security Loss (1st Party Intangible/Information), Network Security Business Interruption Coverage (1st Party), a Cyber Criminal Reward Fund, and a Crisis Communication Management Fund. www.aignetadvantage.com. *Id.* The Chubb Group of Insurance Companies recently announced it will offer scalable coverage for information and network technology companies. *Id.* The Chubb INTegrity policy will insure against the risks of loss associated with contractual Definitions of Loss, Final Acceptance Criteria, Privacy Violations, Intellectual Property Infringement, and Security Breach by Others. *Id.*

been created by the venture must be considered the intellectual property of others. The non-lawful use of the intellectual property of others invites "bet-the-business" litigation. Certain industry practices in vogue, "data-mining" in particular, are intellectual property liability traps for the unwary.

2. The medical software venture must operate a rigorous intellectual property recognition and protection program. All documents and data related to the medical software should be treated as if they were trade secrets. Hard copies should be strictly accounted for and physically safeguarded, and electronic documents and databases should be physically guarded, encrypted, and subject to password protection. All software-related information and data created by the venture, in both hard copy and electronic versions, should be regularly screened and classified for the type of intellectual property protection needed. Information or data deserving trade secrets should be given scaled levels of protection. Trade secret data should be segregated into data to be made available to third parties only upon receipt of an executed non-disclosure agreement, with such data effectively being made available on a "need-to-know basis." The venture should conduct a semi-annual marketing survey to attempt to determine whether competitors may be using portions of the medical device software, thereby encroaching on the venture's precious intellectual property rights. Key employees of the venture and all persons having access to the software code must execute written contracts containing non-disclosure terms and non-compete agreements, to the extent allowed by state law. The venture's scientists, engineers, and researchers should be regularly interviewed to determine what portions of their work they believe are valuable new intellectual property. In all instances, the venture should aggressively protect and defend its intellectual property rights.

3. The medical software venture should seek copyright protection for the medical device software. Copyright protection provides an additional measure or protection for abstract and creative content. Copyright protection extends for a longer term. Copyright protection begins at the time the software algorithm is placed on a tangible medium.

4. The venture must determine whether it will seek patent protection for the medical software. Despite its higher cost, patent protection might provide a host of business advantages and benefits. Patent protection for medical software would allow the software to be more widely distributed in the broader market. Patent protection for the medical software could serve as the anchor for a portfolio of related intellectual properties. Prospective purchasers or licensees of the code and the venture will be more likely to act knowing the code was the subject of a grant of a valid patent. The pre-requisite "Freedom to Practice/Non-Infringement" letter from intellectual property counsel can be used as baseline to monitor the actions of competitors.

5. The FDA medical software validation process must be very carefully structured and managed. An "FDA Approval Committee," comprised of the chief executive, the chief technologist, the chief medical expert, and general counsel, should be appointed to serve for the life of the FDA approval process. The committee should review each document to be submitted to the FDA for the presence of non-excised trade secret information. Each document to be submitted to the FDA should be individually numbered and indexed. Any document that must be submitted to the FDA that cannot be "scrubbed" to remove or disguise trade secret information should

carry the following legend: "This document contains Trade Secret data proprietary to (the name of the venture). Federal law prohibits disclosure of this document or data contained in the document to anyone other than FDA personnel or third-party certification personnel. 21 CFR 20.61"

6. Respecting day-to-day operational concerns, the medical software venture must thrive on an inter-related set of strategic policies. Agreements governing the efforts to create, license, lease, or assign medical software must be the subject of negotiation and review by competent counsel. The venture must maintain a comprehensive portfolio of products liability, errors, omissions, and intellectual property insurance coverage. The venture should also dedicate of a portion of its revenues to fund its intellectual property recognition, protection, and enforcement program. The venture should retain litigation counsel on a standby basis.

CONCLUSION

The lawyer in the rich, demanding, rapidly changing medical device software business environment needs to do more than appreciate the strategic importance of a diverse set of laws and circumstances relevant to his or her client's interests. Your clients are treading in the outer boundaries of technology, business, and law. Your task is to ground their optimism, will, purpose, and extraordinary competence with your knowledge of the risks and opportunities presented to them.