

Protecting Intellectual Property in Electronic Medical Record Software

I. Introduction

A. Health Care and the Electronic Medical Record

In recent years, health care in the United States has undergone a drastic change. Many hospitals that were once decentralized and self-sustaining organizations have integrated into large corporate entities that consolidate most business concerns and management structures. As efforts to boost efficiency continue, corporate development has increased.¹ Today's health care system may purport to offer patient care along a continuum in a variety of inpatient and outpatient settings and at different points of need.² The modern health care system may be a corporation operating for-profit or not-for-profit,³ and as such may own complex real property as well as physician practices. It may be subdivided into subsidiaries and may even operate its own insurance company. In all aspects, the health care corporation is a sophisticated entity.⁴

Trotting alongside this drastic change in organizational structure is a continual improvement in medically related technology. The United States is known for its desire to have and for its ability to create the best in technology.⁵ For example, as early as the 1960s, hospital systems were attempting to transform all paper based clinical documentation and scheduling processes, (the medical record), into an electronic version

¹ Paul Starr, *Elements of the Corporate Transformation of Medicine* in *A Health Law Reader: An Interdisciplinary Approach*, (John H. Robinson, Roberta M. Berry and Kevin McDonnell, editors), (1999) at 505.

² *Id.* at 506 (describing a phenomena known as vertical integration).

³ *Id.* at 505.

⁴ *Id.* at 505,506, (and, for example see UPMC, University of Pittsburgh Medical Center, *About UPMC(2004)* at <http://www.upmc.com/Overview.htm>).

⁵ Cinda Becker, *Special Report: The Best Care Money Can Buy; The U.S. Delights in Its Medical Technology, and Pays a Premium for It, but Studies Show Other Countries Beat Us in Outcomes, Value, Modern Healthcare*, August 9, 2004, vol. 34, no. 32, 8/9/04 MODHC 26 at [2004 W.L. 63462738](http://www.modhc.com/2004/W.L.63462738) at 1.

of same.⁶ But, even though the current U.S. Administration has declared that an electronic medical record, (EMR), should be a standard part of American health care within ten years, the same source also estimates that only 13% of this country's hospitals have succeeded in this endeavor and only 50 % to 75% of hospitals will have a functional EMR within ten years.⁷ The creation of a computer-based medical records system is undeniably complicated, requiring a large capital outlay and considerable technical and legal support.⁸

Software is a key component of the EMR and is either purchased, developed in-house and licensed or jointly developed with companies outside the healthcare system.⁹ A multitude of laws impact this dynamic developmental process.¹⁰ Among these are the intellectual property laws whose scope includes four methodologies generally used to legally safeguard the creation and use of EMR software. These are patent protection, copyright protection, trade secret protection and trademark protection.¹¹ Within the structure of these methodologies, it is critical for a health care system to consider how best to safeguard the organization and the EMR software that it fosters or creates. This paper will attempt to define the elements that may lead to a corporate decision making framework for those managing this complex arena.

⁶ Jerome H. Carter, M.D. *Electronic Medical Records: A Guide for Clinicians and Administrators*, (2001), at 7.

⁷ Becker, *supra*, note 5 at 6 and *Newsline Digest – Bush Records Goal a Tough Target*, Health Data Management, vol. 12, no. 8, August 2, 2004, 8/2/04 HDAMGMT 26 at [2004 WL 62524607](#) at 1.

⁸ Margaret Amatayakul, *Making the Case for Electronic Records*, Health Data Management, May 19, 1997, 5/19/97 HDAMGMT at [1997 WL 8747870](#) (no page), at 1.

⁹ Carter, *supra* note 6 at 307, Marion J. Ball, Morris F. Cohen, editors, *Aspects of the Computer-Based Patient Record*, (1992) at 6, 15 and Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care*, (1997) at 216.

¹⁰ Carter, *supra* note 6 at 260-267.

¹¹ Melissa S. Sellers and Tracy-Gene G. Durkin and the Association of Corporate Counsel, *Eternal Sunshine of the Spotless Portfolio: Creating and Implementing an Effective Corporate Intellectual Property Program*, ACC Docket, Nov/Dec, 2004, 22 No. 10 ACC Docket 78 at [22 No. 10 ACCDKT 78](#) at 101.

B. Goals and Organization

This writing is structured to give an interested person a limited overview of legal matters and organizational strategies available to safeguard the development and use of electronic medical record computer software within a health care system.

Section II defines the parameters of a medical record and of an electronic medical record.

Section III provides a synopsis of laws that generally affect medical records and of the intellectual property inherent in software development.

Section IV A-E details substantive elements of each category of intellectual property law and proposes strategies for using these laws to a health care system's advantage.

Section V further summarizes these strategies and Section VI provides concluding remarks.

II. The Medical Record

A. The Medical Record: Definition and Uses

A *medical record* is a multi-faceted, paper oriented entity that contains “information to justify admission and continued hospitalization [or care], support the diagnosis, and describe the patient’s progress and response to medications and services.”¹² The information in the record must be authenticated by proper medical authorities, and the healthcare facility, inpatient or outpatient, must keep one for every patient.¹³ The facility must maintain adequate systems for coding, indexing and timely retrieval of information.¹⁴

¹² 42 C.F.R. §482.24 (3) (2004).

¹³ 42 C.F.R. §482.24 (3) (a-c)(2004).

¹⁴ 42 C.F.R. §482.24 (3) (a-c)(2004).

A medical record is primarily used by the clinician, but may have various uses to healthcare facility management; to laboratory, pharmacy, radiology or other index oriented service systems; and, in the aggregate, to gatherers of statistical public health data.¹⁵

B. The Electronic Medical Record

An *Electronic Medical Record (EMR)* is an improvement on the paper version. It is considered a computer-based, interactive tool for clinical caregivers and decision makers, combining specific and pertinent patient data with general database information, and having unique data storage, configuration, reconfiguration and presentation possibilities.¹⁶ The milieu of a changing healthcare environment, ever more technically oriented, reinforces the need for a computer- based medical record. Advances in technology are partially responsible for the great strides that have been made in health care in recent decades. Computers have made it possible for information from research and care, by minute specificity and also in the aggregate, to be combined and recombined in theoretically unlimited opportunities to view data in new ways. The hope is that a computer-based, or paperless, patient record, will allow improvements in patient care, in productivity, in continuing education and in the satisfaction and safety of patients and caregivers.¹⁷

The trend for hospitals, as noted earlier, has been to merge into complex health systems. Finding a way to harness the power of computer based systems into an EMR and to make use of that EMR across a system that may consist of several once independent hospitals,

¹⁵ Carter, *supra*, note 6 at 6,7.

¹⁶ Carter, *supra*, note 6 at 7,8,9

¹⁷ Amatayakul, *supra* note 8 at 6 and Michael Romano, *Information = Power; Modern Healthcare's Third Annual 100 Most Powerful Ranking Attests to the Prominence of IT, Quality and Patient-Safety Initiatives*, Modern Healthcare, August 23, 2004, vol. 34, no. 34, 8/23/04 MODHC 6 [at 2004 63462813](#), at 2.

clinics and other support corporations is a huge and expensive challenge, costing millions of dollars.¹⁸ The axiom remains that the more computer-based technology that an organization installs, “the more it must invest in support, enhancements and improvements”.¹⁹

The EMR can be a relatively simple, stand-alone product. But to be most useful, it is commonly designed to be more complex and to link with existing computerized systems. The EMR can be integrated for *presentation* purposes or for *data* purposes.²⁰ The former is easier to accomplish than the latter.²¹ *Data integration* allows for query capabilities. Most hospital systems attempt to create an EMR that will aspire to some type of data integration.²² Visions of streamlined and standardized pharmacy ordering and test scheduling, wireless workstations and bedside PCs are tantalizing dreams. But the successful attainment of these goals across all of the entities in a healthcare system involves at least common coding of data and sometimes the breakdown and refabrication of already existing systems.²³

Important elements of the EMR include *hardware*, *databases*, and *data input technologies*, as well as *networking*, *biometrics*, *messaging*, *coding* and *classification* systems.²⁴ While *hardware* involves the physical machines upon which the computer

¹⁸ Ball, *supra* note 9 at 265,268.

¹⁹ John Morrissey, *Capital Crunch Eats Away at IT; Annual Survey Shows Lack of Funding among Obstacles Slowing Adoption of Computerized Physician Order Entry, Other Projects, Modern Healthcare*, Vol. 34, No. 8, 2/23/04 MODHC 32 at [2004 WL 63462025](#) at 2.

²⁰ Carter, *supra* note 6 at 9,10.

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ Carter, *supra* note 6 at 11.

plays out its various functions, *databases* and *database management* systems are *software* programs that permit storage, retrieval and manipulation of information.²⁵

Data input technologies allow a person to interact with a computer. Most familiar is the now common keyboard and mouse. More *high-tech* options include pen-based technology that allows a user to literally *write onto* the computer as well as voice recognition technology in which a computer can be trained to translate a user's verbal inputs and commands.²⁶

Networking, once a practice of hard-wiring computers together to form a system that could communicate, now generally involves the *internet*.²⁷ The *internet* as a networking tool only requires a main computer, or *server* and a software program called a *browser*. The browser program is written in such a way that it communicates with the internet and can send and receive information from any browser, often using telephone lines. When specific browser/server systems limit access to certain people with a collection of specific functions, the networking mechanism is called an *intranet*.

Wireless network systems that rely on radio frequencies are becoming more popular and available. Such systems allow for the freedom to move hardware, such as PCs, from place to place as needed.²⁸

Security is always an issue with the sensitive components of an EMR. Most organizations with computers use passwords to guard access. Now, *biologic markers*,

²⁵ *Id.*

²⁶ Carter, *supra* note 6 at 11,12.

²⁷ Carter, *supra* note 6 at 12, 13.

²⁸ *Id.*

like fingerprint and iris scanning programs as well as face and voice recognition programs are technologically available.²⁹

With an EMR, *clinical storage information* systems involve sophisticated technologies for the movement of information between subsystems as well as methods for *messaging, coding* and *classifying* data. Standardization is critical in these methodologies.³⁰

III. Legal Issues in General

The creation of an EMR is an endeavor that sometimes takes years in a large healthcare corporation. The security of the systems and the confidentiality required of the data held by the systems create high legal concerns. The software that is necessary to the complex overall system is sometimes purchased outright, sometimes developed over time in cooperation with a vendor and sometimes created in-house. (See I. A, *supra*.) To be better than the static paper record, it is necessary that an EMR remain an evolving endeavor, necessitating an ever changing combination of off- the- shelf plus internally created and protected components. In all such instances, protection of the hardware, the software and of the information created by use of the EMR is essential. Knowledge of the laws that are designed to protect such information and systems is therefore critical.³¹ This paper will concentrate on the laws that the affect intellectual property rights in the hardware and, most specifically, the software of the EMR. To place this subset of laws in context, a brief overview of the other types of laws affecting an electronic medical record system will be offered.

²⁹ Carter, *supra*, note 6 13

³⁰ Carter, *supra*, note 6 at 13-16.

³¹ Institute of Medicine, *supra*, note 9 at 4.

Integrity of patient data is important in avoiding tort liability.³² Data integrity can be affected by deliberate fraud, accident, machine failures or computer hackers.³³ As the EMR is built over time, contract law also comes in to play. Relationships between vendors, consultants and hospitals must be renegotiated at each turn of the evolving invention of an EMR.³⁴

State licensure laws have implications in the shaping of an EMR and may vary across the continuum of services provided and care settings.³⁵ Areas affected by subsequent regulations include those related to the creation, authentication, and storage of medical records.³⁶ “Additional requirements typically found in state licensure statutes relate to confidentiality, record content, accuracy, completeness, timeliness, and accessibility.”³⁷ Federal regulations³⁸ govern the way that a provider like a medical doctor, must utilize, authenticate and safeguard medical records.³⁹ Accrediting bodies, like the Joint Commission on the Accreditation of Healthcare Organizations set some voluntary standards that generally complement state regulations.⁴⁰

³² *Donald R. and Judy Hudson v. Patrick McCarthy, M.D. et al*, No. 80769, 2002 WL 31261001 (Ohio App. 8 Dist.) (2002) at 3.

³³ *Hudson v. McCarthy, M.D. et al*, 2002 WL 31261001 (Ohio App. 8 Dist.) *supra*, (as an example of fraud), *Lambrech and Associates, inc. v. State Farm Lloyds*, No. 12-01-00146-CV, 119 S.W. 3d 16, (2003) (for a discussion of necessity to protect against computer hackers), and *Technology is changing the Health Data Security Landscape*, Health Data Management, September 19, 1997, 9/19/97 HDAMGMT (No Page) at [1997 WL 8747994](#) at 1,3 and John Morrissey, *Information Edge: Boosting IT Immunity; Expanding Computer Networks and Widespread Use of the Internet Leave Healthcare Systems Highly Vulnerable to Viral Attacks*, Modern Healthcare, February 23, 2004, vol. 34, no. 8, 2/23/04 MODHC 40 at [2004 WL 63462034](#) at 1.

³⁴ Institute of Medicine, *supra*, note 9 at 219-221.

³⁵ *Id.* at 200, 201.

³⁶ *Id.* at 201.

³⁷ *Id.* at 201.

³⁸ 42 C.F.R. §482 et seq. (2004)

³⁹ Institute of Medicine, *supra* at 207.

⁴⁰ JCAHO, Hospital Accreditation Standards, *Standards, Rationale, and Elements of Performance for I.M. 6.10 – I.M. 6.60* (2004) at 284-289.

The Federal Privacy Act of 1974 applies only to federal agencies and health care facilities and limits disclosure of medical record information by federal agencies, requires reporting on disclosures of the existence of information in which a patient may be identifiable and allows patients access to their own records.⁴¹ The Health Insurance Portability and Accountability Act (HIPAA) has been called the most significant legislation related to an EMR.⁴² The statute sets strict standards for users of individually identifiable health information in any form and penalties for misuse.⁴³ The law also mandates special regulations aimed at protecting the security of computerized patient information.⁴⁴

Generally, it is acknowledged that a patient has a degree of property interest in the information contained in his or her medical record and that the provider owns the physical record, as business documentation, with no license to use that information other than what the patient agrees to release.⁴⁵ Health care records are often brought into litigation for their evidentiary value. The rules of evidence that are most often called into play when a record is brought to court are the federal *hearsay* rule, the *business record exception* to the hearsay rule and the *best evidence* rule as well as their state counterparts.

⁴⁶ Any part of a medical record containing contested statements is not a first-hand account but a secondhand account, (technically *hearsay*), requiring separate justification

⁴¹ Carter, *supra*, note 6 at 263 and 5 U.S.C. §552 (2004).

⁴² Carter, *supra*, note 6 at 263.

⁴³ The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

⁴⁴ Bill Siwicki, *Overcoming Electronic Records Hurdles*, Health Data Management, May, 19, 1998, 5/19/98 HDAMGMT (No Page) at [1998 WL 10160980](#) at 7.

⁴⁵ Institute of Medicine, *supra*, note 9 at 211 and Amatayakul, *supra* at 4.

⁴⁶ Institute of Medicine, *supra*, note 9 at 212,213, and 214, See Fed. R. Evid. 801, (2003-2004 edition), Fed. R. Evid. 803 (6), (2003-2004 edition), See Fed. R. Evid. 1002, (2003-2004 edition).

to be heard in court.⁴⁷ Hearsay is not admissible in court unless an exception applies.⁴⁸ But, if the information in a medical record is kept in the regular course of business and not prepared in anticipation of litigation, it may be admissible under the *business record* exception to the hearsay rule.⁴⁹ Sometimes, as the *best evidence* of a matter, the original record must be produced at trial.⁵⁰ Computer generated EMR printouts can sometimes be deemed original records.⁵¹ As healthcare litigation is a costly and common occurrence, these evidentiary matters should be kept in mind when components of an EMR are designed and improved.

IV. Intellectual Property Law and EMR Software Development

A. Overview

Computer *hardware* and *software* must work hand-in-hand to produce an effective EMR system.⁵² *Hardware* represents the physical components of the device⁵³ and *software* refers to the programs, and procedures by which the computer system operates.⁵⁴ As an inventor, a health care system on an EMR quest will most probably be involved at some level with the creation of EMR software products. Once a healthcare system has invested millions in EMR software and software development, it will logically wish to protect it from unlawful duplication.⁵⁵ It may be able to do so by defining the software as

⁴⁷ *Greg Merrow et al v. Diane Bofferding et al*, Docket Nos. 106331, 106332, Calendar No. 8, 458 Mich. 617 (1998) at 701.

⁴⁸ Fed R. Evid. 802 (2003-2004 edition).

⁴⁹ Fed. R. Evid. 803 (6), (2003-2004 edition), (and see, for example) *Timothy Parker v. Commonwealth of Virginia*, Record No. 2017-02-2, 41 Va. App. 643 (2003) at 649,652.

⁵⁰ Fed. R. Evid. 1002, (2003-2004 edition) (and see for example) *Fred's Stores of Tennessee, inc. v. Erica Brown et al*, No. 2001-CA-01127-COA, 829 So. 2d 1261 (2002) at ¶ 6.

⁵¹ Institute of Medicine, *supra*, note 9 at 211-214.

⁵² Edward R. Hyde, *Legal Protection of Computer Software*, 59 CTBJ 298 (1985) at 299.

⁵³ Merriam-Webster Online Dictionary (Dec., 2004) at <http://www.m-w.com>.

⁵⁴ *Id.*

⁵⁵ Diane M. Sidebottom, *Intellectual Property in Federal Government Contracts: the Past, the Present and one Possible Future*, PUBCONLJ 63, (2003) at 64.

intellectual property. *Intellectual property* is a product of the mind; a commercially valuable asset represented by the idea behind the invention.⁵⁶

Modern intellectual property (IP) laws emanate from the U.S. Constitution, Article I, section 8, clause 8, which gives Congress the power “to promote the progress of science and of the useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries”⁵⁷, and section 8, clause 3, which bestows “the power to regulate Commerce...”.⁵⁸ IP laws allow for the creator of a piece of intellectual property to control the exclusive use that is made of that property for a limited period of time, after which the intellectual property must be made available to the general public for purposes of commercial competition.⁵⁹

The process of granting a patent, registering a copyright or registering a trade secret to cover a piece of software are federal processes, governed by the U.S. Patent and Trademark Office (PTO), the Copyright Office of the Library of Congress and the federal court system.⁶⁰ Matters related to unfair competition, the ownership of and contracts related to patents, copyrights and/or trademarks and trade secrets, are generally governed by state law.⁶¹ All of the federal intellectual property statutes are aimed at encouraging innovations and offering the benefits of those innovations to society.⁶² Discussion of each of the major areas of intellectual property law follows. Although there are international implications for each area, this paper will deal primarily with domestic

⁵⁶ Black’s Law Dictionary, abridged seventh edition, Bryan A. Garner, (Editor-in-Chief)(2000) at 649.

⁵⁷ U.S. Const., Art. I, sec. 8, cl. 8.

⁵⁸ U.S. Const., Art. I, sec. 8, cl.3.

⁵⁹ Dana Schilling, Lawyer’s Deskbook- 11th edition, (2000) at 12-1.

⁶⁰ Donald Chisum, Craig Nard, Herbert Schwartz, Pauline Newman and F. Scott Kieff, Principles of Patent Law: Cases and Materials (2004) at 23, 31.

⁶¹ Arthur R. Miller and Michael H. Davis, Intellectual Property: Patents, Trademarks, and Copyright, 3rd ed. (2000) at 150 – 152, 157-162.

⁶² Schilling, *supra*, note 59 at 12-1.

applications of the laws. Under intellectual property laws, protection of innovations can be accomplished by matching the appropriate legal standard to the type of invention or even by using a combination of the protections available under the patent, copyright, trademark or trade secret laws.⁶³

B. Protection of EMR Software through Patents

1. Can EMR Computer Software Be Patented?

The grant of a *patent* for an innovative piece of EMR software will perhaps provide the most unqualified intellectual property protection⁶⁴ but it can be the most expensive and difficult road to take.⁶⁵

A *patent* is a tool that gives the patentee the right to stop others from “making, using, offering for sale, or selling the [the patentee’s] invention throughout the United States [...]or importing into the United States” the product protected by the patent or the product made by the process protected by the patent.⁶⁶ The patent gives the patentee a limited monopoly for a period of 20 years from the filing date of the patent application.⁶⁷

Title 35 of the United States Code encompasses the laws concerning patents and patentability.⁶⁸ A work under this scheme would receive protection via a *utility patent* in one of four types of inventions or discoveries: machines, human made products, compositions of matter, and processing methods. These four types are defined statutorily as patentable subject matter.⁶⁹ A law of nature, a naturally occurring physical phenomena or an abstract idea like an algorithm have all consistently been held by the

⁶³ Hyde, *supra*, note 52 at 319.

⁶⁴ Schilling, *supra*, note 59 at 12-1.

⁶⁵ Hyde, *supra*, note 52 at 314.

⁶⁶ 35 U.S.C. §154 (a)(1)(1994)

⁶⁷ 35 U.S.C. §154 (1994) as referenced in Chisum et al, *supra* at 3. The time period relates to applications filed on or before June 8, 1995.

⁶⁸ 35 U.S.C. §100 et seq. (2004)(effective November 29, 1999)

⁶⁹ 35 U.S.C.A. §101(2004).

courts as not patentable subject matter.⁷⁰ *Utility* means to demonstrate that a product or a process can indeed be expected to be made from the description inherent in the patent application.⁷¹ *Design patents* can also be sought through the application process.⁷² To be patentable, the invention must be *useful*⁷³, *novel*⁷⁴ and *non-obvious*, (not an obvious extension of current technology), at the time of the invention to a person with ordinary skill in the field of the invention.⁷⁵ Part of the *novelty* determination includes the rule that the invention cannot have been known, sold or used by others in the U.S. or described in a written publication anywhere in the world more than one year prior to the U.S. patent application.⁷⁶ The invention must also fit into one of the categories of statutorily patentable subject matter.⁷⁷ In fact, the determination of software patentability revolves around this issue.⁷⁸

After examination by a patent examiner for the above qualities, a long and difficult process, a patent may be granted from the Patent and Trademark Office, (PTO), the federal agency whose responsibility is to administer patent laws.⁷⁹ It wasn't until the 1970's that the PTO and the courts began to issue opinions on the patentability of computer related inventions.⁸⁰ Although it is now firmly established that computer software fits the categorical definition of statutorily patentable subject matter, the concept

⁷⁰ *Parker v. Flook*, 437 U.S. 584 (1978) at 589 and *Gottschalk v. Benson*, 409 U.S. 63, (1972) at 67.

⁷¹ *Miller supra*, note 61 at 69, 70.

⁷² *Id.* at 38.

⁷³ 35 U.S.C.A. §101 (2004).

⁷⁴ 35 U.S.C.A. §102 (2004) (effective November 2, 2002).

⁷⁵ 35 U.S.C.A. §103 (2004) (effective November 29, 1999).

⁷⁶ 35 U.S.C.A. §102 (2004) (effective November 2, 2002)..

⁷⁷ 35 U.S.C.A. §101 (2004).

⁷⁸ *Diamond v. Diehr*, 450 U.S. 175, (1981) at 191,192,193

⁷⁹ *Chisum, supra*, note 60 at 31.

⁸⁰ See *Gottschalk v. Benson*, 409 U.S. 63, *supra*, note 70.

was controversial and vigorously debated in the courts for almost 30 years.⁸¹ A limited evolutionary history may be illustrative.

An expansive Supreme Court, not happy with placing restrictions on innovation, noted in *Diamond v. Chakrabarty*, 447 U.S. 363, (1980) that the statutory classes of patentable inventions could “include anything under the sun that is made by man”⁸², but still limited patentable subject matter by stating that “laws of nature, physical phenomenon, and abstract ideas have been held not patentable”.⁸³

In *Gottshalk v. Benson*, 409 U.S. 63 (1972), the validity of a patent for a methodology for using number conversion in conjunction with a digital computer was questioned. The court said that the concept of what amounted to a computer program was merely a formulaic idea and not tangible. To be patentable, an idea had to be linked to a “substantial practical application”.⁸⁴ It is never possible to know if a mental process, such as a mathematical formula, is *novel* as required by statute.⁸⁵

In a 1978 case, *Parker v Flook*, 437 U.S. 584 (1978), discussion centered on a mathematical formula to calculate an alarm limit value as part of a manufacturing process. But the Supreme Court was still not convinced and effected the denial of a patent to what they considered to be just an algorithm or a formula.⁸⁶ In 1981, in *Diamond v. Diehr*, 450 U.S. 175, (1981) the decisions of lower courts concerning a similar invention, but with a computer and computer program designed to constantly update and correct for the temperature in a rubber mold were reviewed at the Supreme

⁸¹ Julie E. Cohen and Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 Cal. L. Rev. 1, (2001) at 3,4.

⁸² *Diamond v. Chakrabarty*, 447 U.S. 303 (1980) at 309 citing S. Rep.No. 1979, 82d Cong, 2d Sess.,5 (1952) and H.R. Rep. No. 1923, 82d Cong., 2d Sess., 6 (1952).

⁸³ *Id.*

⁸⁴ *Gottschalk v. Benson*, *supra*, note 70 at 71.

⁸⁵ *Id.*

⁸⁶ *Parker v. Flook*, *supra*, note 70 at 586, 596.

Court level. “We have before us today only the question of whether respondents’ claims fall within the section 101 categories of possibly patentable subject matter. We view respondents’ claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula.”, said the court, decreeing that the computer program was a “process”, patentable under 35 U.S.C. section 101.⁸⁷

Following the decisions in *Diehr* the courts faced more and more computer related challenges. In a case called *In re Rene K. Pardo and Remy Landau*, 684 F. 2d 912 (1982), the Court of Customs and Patent Appeals (the precursor to the PTO)⁸⁸ noted a two-part test that became known as the *Freeman-Walter-Abele* test articulating the test as follows:

First, the claim is analyzed to determine whether a mathematical algorithm is directly or indirectly recited. Next, if a mathematical algorithm is found, the claim as a whole is further analyzed to determine whether the algorithm is “applied in any manner to physical elements or process steps,” and if it is, it “passes muster” under §101.⁸⁹

Later, in 1994, a federal court of appeals said in the case of *In re Kurippan Alappat et al*, 33 F. 3d. 1526, (1994) that mathematical algorithms are not patentable unless the abstract idea is reduced to some type of practical application; “a useful, concrete and tangible result.”⁹⁰ This case, and a case called *State Street Bank and Trust Co. v. Signature*

⁸⁷ *Diamond v. Diehr*, 450 U.S. 175, *supra*, note 78 at 191,192,193.

⁸⁸ Chisum et al, *supra*, note 60 at 26, n. 101

⁸⁹ *In re Rene K. Pardo and Remy Landau*, 684 F. 2d 912 (1982) at 915, citing *In re Freeman*, 573 F. 2d 1237 (1978) and quoting modifications by *In re Walker*, 618 F. 2d 758 (1980) and noting conforming decisions in *Diamond v. Diehr*, 450 U.S. 175, *In re Abele*, --F. 2d --No. 81-618 (1982) and *In re Taner*, 681 F. 2d 787 (1982).

⁹⁰ *In re Kuriappan P. Alappat, Edward E. Averill and James G. Larsen, No. 92-1381*, 33 F. 3d. 1526 (1994) at 1544.

Financial Group, inc., 149 F. 3d. 1368, (1998)⁹¹, in effect, rendered the *Walter-Freeman-Abele* test obsolete.⁹²

In *State Street*, a piece of financial management software called the “Hub and Spoke” was patented and assigned to the Signature Financial Group. In an action by State Street Bank, the validity of the patent was challenged on the grounds that the software for business methodology was not proper subject matter for patentability under 35 U.S.C. section 101.⁹³ The court said that the claims described a data processing system as a “machine” or a “means”, both acceptable section 101 statutory subject matter.⁹⁴

Arguments that the system at issue was unpatentable as a “business method exception” were dismissed as based on dicta only⁹⁵, quoting federal guidelines for examiners, which read in pertinent part:

Office personnel have had difficulty in properly treating claims directed to doing business. Claims should not be characterized as methods of doing business. Instead, such Claims should be treated like any other process claims.⁹⁶

The court also swept aside arguments that the system was a mere mathematical formula/algorithm/abstract idea and therefore unpatentable. The court pronounced that the new test for patentability must be one of “practical utility”, and announced that the software patent held by Signature had a practical utility, even though expressed in numbers.⁹⁷

⁹¹ *State Street Bank and Trust Co. v. Signature Financial Group, inc.*, 149 F. 3d 1368 (1998).

⁹² *In re. Alappat*, (33 F. 3d, 1526), *supra*, note 90 and *State Street Bank v. Signature*, (149 F. 3d. 1368), *supra*, note 91.

⁹³ *State Street Bank v. Signature*, (149 F. 3d. 1368), *supra*, note 91 at 1369.

⁹⁴ *Id.* at 1371, 1372.

⁹⁵ *Id.* at 1375

⁹⁶ The U.S. Patent and Trademark Examination Guidelines, 61 Fed. Reg. 7478 (1996) at 7479.

⁹⁷ *State Street Bank. v. Signature supra*, note 91 at 1377.

The patenting of software and other inventions within a university hospital setting, (the type of setting quite likely to develop an EMR), got a boost in the 1980s with the passage of the University and Small Business Patent Procedures Act, also known as the Bayh-Dole Act after the two senators who sponsored it.⁹⁸ When the Bayh-Dole Act was first passed into law, the interests of the nation's academicians in patenting their work was increasing and most university research had some government support. But the question of who really owned government sponsored research; the public who paid for it, or the person who created it, remained. At the same time, new technology-based private businesses, (many of them computer software related), seeing the potential for unprecedented growth, began to sponsor university research themselves and pushed to develop intellectual property rights in what they had helped to fund. But the American economy was facing difficult times and competing opinions at the executive level of the U.S. government led to chaotic law, chilling incentives for inventors and thwarting economic growth linked to scientific inventions.⁹⁹ With no guarantee that they would get exclusivity to manufacture and market the products ensuing from intellectual development, many private businesses stopped trying. Valuable technologies were left at universities or as the property of the government, neither of which functioned in a commercial mode. As a result, technology was not always transferred into use.¹⁰⁰ The Bayh-Dole Act was intended to break this deadlock by promoting efficient commercialization of research and by bringing all government agencies that issued

⁹⁸ 35 U.S.C. §§200-212 (2004) (Effective November 1, 2000) and Corynne McSherry, *Who Owns Academic Work: Battling for the Control of Intellectual Property* (2001) at 150 and Coe A. Bloomberg, *Federal Funded Inventions and Bayh-Dole Act Compliance: Do You Really Own What You Think You Own?* 16 No. 2 JPROPR 1 (Feb. 2004) at 1.

⁹⁹ McSherry, *supra* at 147-150.

¹⁰⁰ Sidebottom, *supra*, note 55 at 65.

patents and licenses under a uniform system of policies and procedures. For government sponsored research and inventions, the act mandates the sharing of profits with inventors as a further incentive to fostering innovation.¹⁰¹

The Bayh-Dole Act has been successful in meeting its goals. Although plagued by new problems and a surge of noncompliance¹⁰², contractors with the federal government are generally retaining commercial rights to their inventions,¹⁰³ and the number of patents that have been issued to universities as well as the number of companies that have been started based on these inventions have increased dramatically since 1980.¹⁰⁴ The number of software patents sought and the number issued have more than doubled from 1987 to 1992.¹⁰⁵

2. How Can Software Patents be Protected?

An organization interested in patenting software that it creates for an EMR must ask if patenting is the right approach. Once the patent application is completed, processing time, (*prosecution*) of the application itself, takes an average of 24.6 months¹⁰⁶ Once patenting has been decided upon as a course of action, the organization should consider options, like those described below, for protecting the patent.

¹⁰¹ 35 U.S.C.A. §202 (2004) (effective November 1, 2000).

¹⁰² Coe A. Bloomberg, *Federal Funded Inventions and Bayh-Dole Act Compliance: Do You Really Own What You Think You Own?* 16 No. 2 JPROPR 1 (Feb. 2004) at 5.

¹⁰³ Jeffrey R. Armstrong, *Bayh-Dole Under Siege: The Challenge to Federal Patent Policy as a Result of Madey v. Duke University*, 30 JCUL 619 (2004) at 622, 623.

¹⁰⁴ Carl E. Gulbrandsen, *Side Bar: The Bayh-Dole Act and Universities Under the U.S. Patent System*, as cited in Chisum et al, *supra*, note 60 at 801.

¹⁰⁵ David R. Syrowik and Roland J. Cole, *The Software Patent Institute and the Challenge of Software Related Patents*, 73 Mich. B.J. 544 (June, 1994) at 4, citing E-mail message dated April 6, 1993 to one of the authors from Gerald Goldberg, Director of Group 2300 of the Patent Office in reply to an E-mail message of April 5, 1993.

¹⁰⁶ United States Patent and Trademark Office, *How Long Does it Take for a Patent Application to be Processed?* (Aug. 14, 2003) at <http://www.uspto.gov>.

a.) A patent attorney should be consulted at critical junctures. This may be expensive, but may prevent or limit an even more expensive battle over patent rights with competing inventor. One documented source noted that in San Francisco, in 2003, the average cost for noninfringement legal patent advice was between \$20,000 and \$50,000 and the cost for an invalidity opinion was up to \$100,000.¹⁰⁷ In addition, if willful infringement can be proven against a party, that party may have to pay treble damages as well as the other side's attorney's fees.¹⁰⁸ It should also be noted that existing patents can be reexamined again by the PTO, with or without an outsider making challenges.¹⁰⁹

b.) "The most obvious reason that people seek patents is to obtain [...] exclusive rights."¹¹⁰ While challenges can occur, once a patent is issued, the burden of proof is on the challenger to disrupt the patentee's rights. This is a very high hurdle and a "right of presumption" is conferred upon the patentee.¹¹¹ It stands to reason that an obvious way to protect all of the rights conveyed by a patent is to exercise those rights gained and conferred by the ownership of the patent.¹¹²

Once a patent is granted, the patentee has the right to stop another from making, using, offering to sell, selling or importing the patented item in or into the U.S. for a specified number of years.¹¹³ The patentee can protect these rights, prospectively, by suing anyone who violates the rights for infringement. If the infringer has been violating these rights retrospectively, the patentee can also sue for damages and attorney's fees.¹¹⁴ It should be noted that an infringer may be accused of usurping a patentee's rights by making an exact

¹⁰⁷ Chisum, et al, *supra*, note 60, quoting San Francisco Daily Journal, Oct. 28, 2003.

¹⁰⁸ 35 U.S.C.A. §284 (2004), §285 (2004).

¹⁰⁹ Chisum, et al, *supra*, note 60 at 151

¹¹⁰ Syrowik, *supra*, note 105 at 5.

¹¹¹ 35 U.S.C.A §282 (2004) (effective November 2, 2002).

¹¹² Syrowik, *supr*, note 105 at 5.

¹¹³ 35 U.S.C.A. §271(a) (2004) (effective December 8, 2003).

¹¹⁴ 35 U.S.C. §284 (2004), §285 (2004).

duplicate of the patented software, and also, sometimes by making something so nearly similar to the patented item that it is the functional equivalent. The *Doctrine of Equivalents* can be applied in an infringement suit by judging whether the infringing product “performs substantially the same function in substantially the same way to get substantially the same result” as the patented product.¹¹⁵ The Doctrine of Equivalents arguments also work in favor of software patent holder in another way. The Supreme Court in *Warner-Jenkinson Co. v. Hilton Davis Chemical Co.*, 520 U.S. 17 (1997), allowed an alternate test for equivalency that asks whether a skilled practitioner in the relevant field would know about the interchangeability between the patentee’s claimed element and the infringer’s claimed element at the time of the infringement.¹¹⁶ The court also said that the finding (or not) of equivalence is a question of fact for a jury.¹¹⁷ If the alleged infringer can’t prove noninterchangeability, (that his claim is different), the patentee is free to make use of improvements to a greater extent than patent holders in other industries.¹¹⁸

c.) A patent owner can solidify the ownership of a patent by requiring assignment from employee/inventors or contractors, by selling the patent, or by licensing it or by otherwise defining ownership.¹¹⁹ In general, one who invents something owns it.¹²⁰ But an employer can contract with an employee to assign rights in an invention back to the employer.¹²¹ However, even without an express agreement, an employer can still claim

¹¹⁵ Miller, *supra*, note 61 at 128.

¹¹⁶ *Warner-Jenkinson Company, inc. v. Hilton Davis Chemical Co.*, 520 U.S. 17, (1997) at 37.

¹¹⁷ *Id.*

¹¹⁸ Cohen, *supra* note 81 at 16.

¹¹⁹ 35 U.S.C. § 271 (d) (2004) (effective December 8, 2004).

¹²⁰ *J. Michael Teets v. Chromally Gas Turbine Corporation*, Nos. 95-1379, 95-1389, 83 F. 3d 403 (1996) at 407.

¹²¹ *Id.*

ownership of the work when the employee was hired to invent.¹²² Such a work-for-hire arrangement indicates an *implied-in-fact* assignment of ownership rights when the employee's full pay and focus is on invention.¹²³ But to be deemed an implied-in-fact contract, the arrangement must survive a test for 1) a meeting of the minds between employer and employee, 2) showing tacit agreement, 3) as evidenced by the circumstances.¹²⁴ By misrepresenting claims to an employee and not pursuing a company policy to have him sign an assignment agreement, the court in *Gerald Banks v. Unisys Corp.*, 228 F. 3d. 1357 (2000), concluded that there was no implied-in-fact contract for the employer to keep the employee's invention¹²⁵, in essence, failing the test set out in *J. Michael Teets v. Chromally Gas Turbine Corp.*, 83 F. 3d. 403 (1996).

But when all is well between employer and employee, the employer can obtain a common law *shop right* in an employee's invention, allowing the employer to use the invention freely in the interests of equity.¹²⁶

Joint inventorship leads to joint ownership. With supplied evidence, even circumstantial, one who contributed in some measure to an invention gains a pro rata share in a patent.¹²⁷

A patent owner can always sell the patent and all of its inherent rights, thus gaining an asset in exchange, but losing the ability to control use of the software.¹²⁸

It is also important to clarify rights under a licensing agreement. In a licensing agreement, the patentee retains ownership for the life of the patent, but grants an exclusive right to a licensee to do something that is claimed in the patent, (i.e., manufacture or use the

¹²² *Id.*

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ *Gerald Banks et al v. UNISYS Corp., No. 00-1030*, 228 F. 3d 1357(2000), at 1360.

¹²⁶ *Max McElmurry et al v. Arkansas Power and Light Co, No. 92-1246*, 995 F. 2d. 1576 (1993) at 1580.

¹²⁷ *Ethicon, inc. v. United States Surgical Corp.*, 135 F. 3d 1456 (1998), at 1460, 1461, 1472.

¹²⁸ 35 U.S.C. §154 (a)(1) (2004) (effective November 2, 2002).

invention), often in exchange for the payment of a royalty.¹²⁹ It is important for the licensing agreement to involve a discussion about what becomes of improvements to the software while the licensee is using it. Generally, a licensor can require the licensee to “license-back” any improvements made.¹³⁰ These rights may have to be negotiated and renegotiated as software emerges in new formations, especially if the licensing involves a long term arrangement with an outside contractor.

d.) Record keeping is essential to keeping patents safe. Outsiders may challenge the right to be considered the first inventor of the software. Disclosure by employees of patentable ideas backed up by signatures and policies relative to rights and responsibilities mark a good beginning to the establishment and maintenance of ownership. Disclosures and records have value as an organization determines how many resources to put into an idea that may become patentable.¹³¹

It is equally important for an organization to realize what it does not own. Periodic patent searches should be done, not only to keep abreast of technological developments, but to avoid costly infringements on other’s patents. One must submit what it knows about other similar inventions in a patent application.¹³²

Last, it is paramount to keep in mind that with software for an EMR, ownership issues reflect back on the concern that much of the information included in a software database relates confidentially to patients.¹³³

¹²⁹ Schilling, *supra*, note 59 at 12-51, 12-52, Black’s, note 56 at 743 and 35 U.S.C. §271 (d) (2004) (effective December 8, 2003).

¹³⁰ 35 U.S.C. §271(d) (2004) (effective December 8, 2003).

¹³¹ Sellers, *supra*, note 11 at 94, 99.

¹³² *Intellectual Property* (2004) at <http://FindLaw.com> and 35 U.S.C. §102 (2004) (effective November 2, 2002).

¹³³ Carter, *supra*, note 6 at 256.

e.) Perhaps the best way to protect the patent is to prepare the application well, according to all of the standards set forth in the 35 U.S.C. section 101 et seq. As seen from the statute and tests of the statute in the cases above, one must be sure that the invented software is novel, nonobvious, and has some practical, tangible utility.¹³⁴ Hard work on the front end of inventing software will help guard against infringements. For example, as part of the claim of novelty, an inventor must be sure that someone else has not invented the software first. And so, a dedicated search for *prior art*, (other previously patented inventions¹³⁵), is essential.¹³⁶

f.) Although this is a controversial concept, it has been proposed that "[...] one can prevent others from patenting software technology that is vital to his or her business, without the expense of obtaining a patent, by publishing the software technology"¹³⁷ In this way, it is likely to become prior art and not as available to give another an exclusive invention.¹³⁸ In the interest of allowing technology to move forward by making database and software available to the public, a nonprofit project called the Software Patent Institute, (SPI), has been created. The SPI helps to make information about software available to the public and to the PTO.¹³⁹

g.) The Bayh-Dole Act, described earlier, governs the patenting of inventions from government-sponsored research.¹⁴⁰ If an organization has an agreement with a federal agency, e.g., to research or create EMR software, it must disclose the invention and can,

¹³⁴ 35 U.S.C.A. §101 (2004), §102 (2004) (effective November 2, 2003), §103 (2004) (effective November 29, 1999)..

¹³⁵ Black's, *supra*, note 56 at 84.

¹³⁶ Miller, *supra*, note 61 at 72.

¹³⁷ Syrowiak, *supra*, note 105 at 5.

¹³⁸ *Id.*

¹³⁹ Syrowik, *supra*, note 105 at 1.

¹⁴⁰ 35 U.S.C.A. §200 et seq. (2004) (effective November 1, 2000)

in most cases, choose to retain title to the invention.¹⁴¹ But, under certain conditions, (i.e. the inventor does not apply for a patent in a timely manner¹⁴²), the government may *march in* and take back title to the invention.¹⁴³ Therefore, if government funding is part of a scheme for the progression of the EMR, it will be important to pay close attention to Bayh-Dole requirements relative to the patenting of EMR software.

h.) *Reverse engineering* represents another threat to EMR software. *Reverse engineering* refers to the process of examining a product, such as a piece of software, “starting with the known product and working backward to divine the process which aided in its development or manufacture.”¹⁴⁴ Reverse engineering is legal under trade secret law.¹⁴⁵ To some extent, reverse engineering has been tolerated in the area of copyrights¹⁴⁶. But, there is no exception, (like the limitation on exclusive rights in computer programs in copyright law that allows for some reverse engineering)¹⁴⁷, in the patent law of infringement.¹⁴⁸ Therefore, it may be possible to assume that patenting provides some effectiveness as a shield against the reverse engineering of patented EMR software.¹⁴⁹

C. Protection of EMR Software through Copyrights

1. Can EMR Software be Copyrighted?

A *copyright* is a “property right in an original work of authorship (such as literary, musical, artistic, photographic, or film work) fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform, and display

¹⁴¹ 35 U.S.C. A. §202 (2004) (effective November 1, 2000).

¹⁴² *Id.*

¹⁴³ 35 U.S.C.A. §203 (2004) (effective November 1, 2000).

¹⁴⁴ Chisum, *supra*, note 60 at 1191 quoting *Kewanee Oil Co. v. Bicron Corp, No. 73-187*, 416 U.S. 470 (1974) at 476.

¹⁴⁵ *Kewanee Oil Co. v. Bicron Corp, No. 73-187*, 416 U.S. 470 (1974) at 476.

¹⁴⁶ Cohen, *supra*, note 81 at 17, 18.

¹⁴⁷ Cohen, *supra*, note 81 at 18 and 17 U.S.C. §117(2004) (effective October 28, 1998).

¹⁴⁸ 35 U.S.C. §271 (2004) (effective December 8, 2003).

¹⁴⁹ Cohen, *supra*, note 81 at 19.

the work.”¹⁵⁰ Copyright laws are now almost exclusively federal,¹⁵¹ emanating from Article I, clause 8, section 8 of the U.S. Constitution¹⁵², and offering statutory protection at the point in time when an *original work is fixed into a tangible form*.¹⁵³ This federal copyright protection point definition is the general rule since the last enactment, (January 1, 1978), of the U.S. Copyright Act and its revisions.¹⁵⁴ However, the notion of “common-law copyright”, (“a property right that arose when the work was created, rather than published”)¹⁵⁵, remains for common-law copyrights received before January 1, 1978.¹⁵⁶ An additional statute, the Digital Millennium Copyright Act of 1998, considers complex copyright issues, including the circumvention of copyright protection and those involving advanced technologies, including computer software .¹⁵⁷ Within this paper, only the current, (post 1978), copyright laws and protections will be discussed. It should be noted that if federal law does not completely protect software in a copyright, one can turn to state common law remedies against unfair competition and tortious conduct.¹⁵⁸ But, where a state law interferes with federal regulation, the state law will be preempted under the Supremacy Clause of the U.S. Constitution.¹⁵⁹

Copyright protection is grounded in the concepts of *originality* and *expression*.¹⁶⁰

Originality does not have the same rigorous review or standard that *novelty* does under patent law. A copyrighted work can still be deemed *original* as long as the facts do not

¹⁵⁰ Black’s, *supra*, note 56 at 273.

¹⁵¹ 17 U.S.C.A. §§ 101-810, (1976) as noted in *Copyright: An Overview*, Legal Information Institute at <http://www.law.cornell.edu/topics/coopyright.html> and Miller, *supra* note 61 at 288-294.

¹⁵² U.S. Const. Art. I, sec. 8, cl. 8.

¹⁵³ Miller, *supra*, note 61 at 287 and 17 U.S.C. §102(a) (2004).

¹⁵⁴ Miller, *supra*, note 61 at 287.

¹⁵⁵ Black’s, *supra*, note 56 at 273.

¹⁵⁶ Black’s *supra*, note 56 at 273 and Miller, *supra*, note 61 at 281.

¹⁵⁷ 17 U.S.C. §1201 (2004) (effective November 29, 1999).

¹⁵⁸ Miller, *supra*, note 61 at 150 – 152 and 17 U.S.C. §301 (b) (1),(3) (2004) (effective October 27, 1998).

¹⁵⁹ Miller, *supra* at 150, and U.S. Const. Art. VI., sec. 2

¹⁶⁰ Hyde, *supra*, note 52 at 306 and 17 U.S.C. §306 (2004).

indicate that the work was knowingly stolen from someone else. In other words, person B can have an idea some time after person A had the same idea, but if person B did not know of person A's idea, publishes the idea in some fixed form and obtains a copyright, person B would theoretically be able to sustain the copyright.¹⁶¹ In *Fierst Publications, v. Rural Telephone Service Company*, 499 U.S. 340, (1991), the court noted that, “[O]riginality is a constitutionally mandated prerequisite for copyright protection.”¹⁶², that “[...] the originality requirement is not particularly stringent...”, and that even a compilation of known facts can be rearranged with some minimum creativity to meet this standard.¹⁶³

A copyright protects “the expression of ideas in written, musical, visual, filmed, or similar form”.¹⁶⁴ One cannot receive a copyright for a functional item¹⁶⁵ or for an idea by itself.¹⁶⁶ The idea must be embodied, or *expressed*, in some type of fixed form.¹⁶⁷ For example, a dance cannot be copyrighted unless it is filmed or written into some type of coded choreography.¹⁶⁸

To obtain copyright protection, one need only fix the work in question in some type of concrete form, from which the work can be “perceived, reproduced or otherwise communicated.”¹⁶⁹ The work is copyrighted from the point of creation for the life of the

¹⁶¹ *Id.*

¹⁶² *Fierst Publications, inc. v. Rural Telephone Service Co., inc., No. 89-1909*, 499 U.S. 340 (1991) at 351.

¹⁶³ *Id.* at 358.

¹⁶⁴ Schilling, *supra*, note 59 at 12-5.

¹⁶⁵ *Torah Soft Ltd. v. Michael Drosnin et al, No. 00 Civ. 5650 (SAS)*, 136 F. Supp. 2d 276 (2001) at 285.

¹⁶⁶ 17 U.S.C. §102 (b) as follows: “In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.”

¹⁶⁷ Schilling, *supra*, note 59 at 12-5 and Miller, *supra*, note 61 at 306.

¹⁶⁸ Miller, *supra*, note 61 at 306.

¹⁶⁹ 17 U.S.C. § 102(a) (2004)

creator plus 70 years¹⁷⁰. With joint creators, the term is 70 years from the death of the longest living joint creator.¹⁷¹ If the work in question was made for hire and owned by an entity other than the creator, the term of the copyright is the shorter of 95 years from the first publication of the work or 120 years from its first creation.¹⁷²

Although not necessary, a creator can place a *notice of copyright*, such as *Copyright, Copr. or ©*, the date of the first publication and the name of the owner on a work published in the United States.¹⁷³ The notice of copyright serves to diminish an infringer's claim that he unknowingly infringed.¹⁷⁴ Also permissively, the owner of a copyright can submit copies of the work, and register the creation with the U.S. Copyright Office.¹⁷⁵ If a creator expects to bring suit in the United States concerning his work, he must register the work beforehand.¹⁷⁶ An aggrieved party can only recover statutory damages and attorney's fees relative to infringement of a published work if the work is registered within three months of publication and before a suit is brought.¹⁷⁷ In 1980, an amendment to the Copyright Act, 17 U.S.C. section 117, expressly allowed for the copyrightability of computer programs and detailed the boundaries of copyrights on computer programs¹⁷⁸

A *computer program* is defined in 17 U.S.C.A section 101 as, "[...] a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a

¹⁷⁰ 17 U.S.C. § 302(a)(2004) (effective October 27, 1998).

¹⁷¹ 17 U.S.C. § 302(b) (effective October 27, 1998).

¹⁷² 17 U.S.C. § 302(c) (effective October 27, 1998).

¹⁷³ 17 U.S.C. § 401 (a), (b) (2004).

¹⁷⁴ 17 U.S.C. § 401(d) (2004).

¹⁷⁵ 17 U.S.C. § 407(a), (b), (c) (2004).

¹⁷⁶ 17 U.S.C. § 411(a) (2004) (effective October 28, 1998).

¹⁷⁷ 17 U.S.C. § 412 (2004).

¹⁷⁸ Deborah F. Buckman, J.D., *Copyright Protection of Computer Programs*, 180 A.L.R. Fed. 1, (2002-2004) at §2 (a) and 17 U.S.C. §117.

certain result.”¹⁷⁹ The statutory definition of the term *computer program*, under copyright law has been interpreted as meaning both the literal and nonliteral components of the program or the software.¹⁸⁰ “The literal components include the *source code*--code that is in a form readably understandable by the programmer--and the *object code*—code that is understandable to the machine ...”¹⁸¹ Nonliteral components of a computer program include “the sequence, structure, and organization of the program, as well as the screen output or user interface, sometimes called the program’s ‘look and feel’”.¹⁸² Especially with the nonliteral components of a computer program, the way in which the software may be protected will depend on the specific ways in which *expressions* are distinguished from function.¹⁸³ In *Tandy Corporation v. Personal Micro Computers, inc.*, 524 F. Supp. 171(1981), the court stated that “a computer program is a “work of authorship” which is “subject to copyright” and “a silicon chip” is “tangible medium of expression” ...”such as to make a program fixed in that form subject to copyright laws.”¹⁸⁴

Copyright protection can extend to nonliteral components of a computer program, such as audiovisual screen displays or process control packages, if the display or control package can be seen as an artistic expression of the idea behind a program and allows the user some degree of creative option.¹⁸⁵ In the landmark case of *Apple Computer, inc. v. Franklin Computer Corp*, 714 F. 2d 1240 (1983), the court reaffirmed “[...] that a

¹⁷⁹ 17 U.S.C. §101 (2004) (effective November 2, 2002).

¹⁸⁰ Miller, *supra*, note 61 at 311.

¹⁸¹ Miller, *supra*, note 61 at 311,312.

¹⁸² Miller, *supra*, note 61 at 312.

¹⁸³ *Id.*

¹⁸⁴ *Tandy Corporation v. Personal Microcomputers, inc.*, No. C-81-0744 RFP, 524 F. Supp. 171 (1981) at 173.

¹⁸⁵ *Broderbund Software, inc. v. Unison World, inc.* No. C-85-3457 WHO, 648 F. Supp. 1127 (1986), at 1133 and *Johnson Controls, inc. v. Phoenix Control Systems, inc.* No. 87-15088, 886 F. 2d. 1173 (1989) at 1175.

computer program in object code embedded in a ROM chip is an appropriate subject of copyright.”¹⁸⁶ However, even a fixed expression of an idea in a computer program must be analyzed to determine if the expression is standard in the industry and if the expression as such is merely applied to knowledge that is already in the public domain, in which case, copyright protection may be denied.¹⁸⁷ A menu command system, may also be precluded from copyright protection as a method of operation.¹⁸⁸

If there are only a few ways to express an idea such that the idea and the expression are virtually indistinguishable from each other they are said to *merge*, and copyright protection is not available.¹⁸⁹ In the area of computer software the *merger doctrine* is sometimes invoked to prove that infringement could not have occurred because the software was never copyrightable subject.¹⁹⁰

Additional protections for computer technology are provided by the Semiconductor Chip Act of 1984, 17 U.S.C. sections 902 et seq.¹⁹¹ The act combines patent and copyright law to protect computer code existing as circuitry in a computer chip, such as ROM (read-only-memory) chips.¹⁹² The chip is eligible for protection from reproduction, distribution or importation by anyone but the owner from the date of registration of the chip or from the date of the first commercial use, whichever is earlier.¹⁹³ But, it is usually not a violation to reverse engineer the program embodied in the chip.¹⁹⁴

¹⁸⁶ *Apple Computer, inc. v. Franklin Computer Corporation*, No. 82-1582, 714 F. 2d 1240 (1983) at 1249

¹⁸⁷ *Torah Soft v Drosnin*, 136 F. Supp. 2d. 276, *supra*, note 165 at 289, 290, (discussing a matrix format display of information found in the Bible).

¹⁸⁸ *Lotus Development Corp. v. Borland International, inc. No. 93-2214*, 49 F. 3d 807 (1995) at 815 and 17 U.S.C. §102 (b) (2004).

¹⁸⁹ *Baker v. Selden*, 101 U.S. 99, (1879) at 104, 105. (credited as first articulating the doctrine of merger).

¹⁹⁰ *Torah Soft v. Drosnin*, 136 F. Supp. 2d 276 (2001), *supra*, note 165 at 283, 284, 285.

¹⁹¹ 17 U.S.C. §§902 et seq (2004).

¹⁹² Miller, *supra*, note 61 at 314, 315 and 17 U.S.C. § 902 (b), (c) (2004).

¹⁹³ 17 U.S.C. §902 (a)(1)(A) (2004).

¹⁹⁴ Miller, *supra*, note 61 at 315.

With a few limitations¹⁹⁵, the owner of a copyright has the exclusive right:

- To reproduce the copyrightable work,
- To make derivative works,
- To give, sell, rent or lease copies of the copyrighted work to anyone else,
- To perform the copyrighted work, (if of a type that is appropriate for such activity),
- To display the work publicly,
- And if the work involves a sound recording, to perform the copyrighted work using audio transmission.¹⁹⁶

If a person other than the copyright owner employs any of the above rights, even unintentionally, without the permission of the copyright owner and without a legally recognized defense, infringement occurs.¹⁹⁷

2. How can Copyrighted EMR Software be Protected?

a) To make the most of copyrights, ownership and defenses to infringement claims must be considered in tandem. In a claim for copyright infringement, the claimant must prove that she owns the valid copyright and that the infringer copied protected and original elements of the work in question.¹⁹⁸ As discussed earlier, it is sometimes possible to prove that a copyright of a computer program was infringed even if the nonliteral elements of the program were the object of the copying.¹⁹⁹ But the difference between a copyrighted expression and the noncopyrightable idea behind it is often difficult to

¹⁹⁵ See 17 U.S.C. §107(2004) (detailing fair use) and 17 U.S.C. §117 (2004)(effective October 28, 1998) (detailing other limitations on the exclusive rights of a computer program related copyright owner).

¹⁹⁶ 17 U.S.C. §106.

¹⁹⁷ Miller, *supra*, note 61 at 340, 355.

¹⁹⁸ *Torah Soft v. Drosnin*, 136 F. Supp. 2d. 276, *supra*, note 165 at 282, *Fierst v. Rural Telephone*, 499 U.S. 340, *supra*, note 162 at 361 and *Harper & Row, Publishers, inc. et al v. Nation Enterprises, et al*, 471 U.S. 539 (1985) at 548.

¹⁹⁹ *Johnson Controls v. Phoenix*, 886 F. 2d. 1173, *supra*, note 185 at 1175.

determine, especially with computer programs.²⁰⁰ A copyright can be infringed by outright, obvious copying of an original work or by creating a very similar work.²⁰¹ An accusation of infringement of either type gains credibility if the alleged infringer had access to the copyrighted work.²⁰²

Common defenses to copyright infringement include ownership²⁰³, the doctrine of *scenes a faire*²⁰⁴, and the doctrine of *fair use* (including allowable reverse engineering).²⁰⁵

Litigating an infringement is highly fact determinative and sometimes necessitates the use of costly expert witnesses.²⁰⁶

The categories of copyrightable material that can be owned are noted in a nonexclusive statutory list.²⁰⁷

b.) Relative to ownership, it is especially important to have a written understanding with employees and contractors.²⁰⁸ Elements of computer programming that are industry standards (as for compatibility) or are external to the program itself are not copyrightable under the doctrine of *scenes a faire*.²⁰⁹

The *Fair Use Doctrine* as described by statute, allows for some reproduction of copyrighted work for limited uses such as critiques, teaching and research.²¹⁰ The statute also outlines factors to be considered in arguing the fair use of copying. These factors

²⁰⁰ *Atari, inc. v. North American Philips Consumer Electronic Corp. et al*, No. 81-2920, 672 F. 2d. 607 (1982) at 615.

²⁰¹ *Original Appalachian Artworks, inc. v. The Toy Loft, inc.*, No. 81-7214, 684 F. 2d. 821 (1982) at 829 FN 11.

²⁰² *Id.* at 829.

²⁰³ 17 U.S.C. §102 (2004).

²⁰⁴ *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*, F. 3d. 823 (1993) at 838.

²⁰⁵ 17 U.S.C. §107 (2004).

²⁰⁶ Miller, *supra*, note 61 at 342-346.

²⁰⁷ 17 U.S.C. § 102(a) (1) – (8) (2004) (Computer software is not specifically noted but the list is not all-inclusive.)

²⁰⁸ 17 U.S.C. §201 (b) (2004).

²⁰⁹ *Gates v. Bando*, F. 3d 823 (1993) *supra* at 838 and *Mitel, inc. v. Iqtel, inc.*, Civ. A. No. 95-B-900, 896 F. Supp. 1050, (1995) at 1056.

²¹⁰ 17 U.S.C. §107 (2004).

include why the work is being copied, whether the use involves a commercial enterprise, what kind of work is being copied, (including the market value of the work), and the extent to which the work is copied in whole or in part.²¹¹

In a landmark case, *Sony Computer Entertainment, inc. v. Connectix Corporation*, 203 F. 3d. 596 (2000), a federal court of appeals ruled that Connectix was employing acceptable fair use when it made intermediate copies of Sony's copyrighted software for operating its *PlayStation*.²¹² Connectix made these copies to determine how the *PlayStation* operating software worked and used this knowledge to make the competitive *Virtual Game Station* product that did not contain any of the Sony *PlayStation* copyrighted material.²¹³ The court, in effect, sanctioned reverse engineering of copyrighted material in order to create a competitive, non-infringing product.²¹⁴ But, a federal court in a more recent case, *Davidson & Associates v. Internet Gateway*, 334 F. Supp. 2d, 1164 (2004), found that defendants had breached a licensing agreement not to reverse engineer computer software when they had explicitly agreed not to do so²¹⁵ and when the end product of that effort was an exact duplicate of the software.²¹⁶ Courts continue to declare that fair use as a defense is highly fact determinative and must be reviewed flexibly so that the stifling of creativity can be avoided.²¹⁷

²¹¹ 17 U.S.C. § 107(2004).

²¹² *Sony Computer Entertainment, inc. et al v. Connectix Corporation*, No. 99-15852, 203 F. 3d. 596 (2000) at 599.

²¹³ *Id.* at 598.

²¹⁴ *Id.* at 599.

²¹⁵ *Davidson & Associates, inc, et al v. Internet Gateway, et al*, No. 4:02-CV-498-CAS, 334 F. Supp. 2d 1164 (2004) at 1178 and 1187.

²¹⁶ *Id.* at 1185.

²¹⁷ *Evolution, inc. v. Suntrust Bank, et al*, No. CIV. A. 01-2409-CM, F. Supp. 2d ,(2004) WL 2271776 (Section III A. 2, no page references available).

c.) The copyright process appears to be less expensive than the patenting process at the outset, involving only permissive registration.²¹⁸ A simple notice of copyright provides further evidence of ownership.²¹⁹ A copyright offers long-lasting protection,²²⁰ but there are ways to get around a copyright, especially in the area of computer programming.²²¹ Not all elements of a work are copyrightable,²²² and the value of vigorously prosecuting infringements, in terms of resources required for such actions, should be evaluated with every case.

d.) It stands to reason that if copyright is desired, an effort should be made to compare the created work to the statutory categories²²³ and, if there is a match, to register and mark the work as copyrighted. For those elements of EMR software that can't be clearly protected, corporate security measures should be a mandate. Not only must copyrighted elements be protected from theft, but the medical record information that may be linked to the copyrighted software must be safeguarded for a variety of reasons.²²⁴

e.) Clear work-for-hire policies should be implemented and licensing agreements that do not violate the copyright statutes should be utilized wherever possible. When a person is hired to create, and unless the employer/employee or the employer/contractor have agreed otherwise, the employer is considered the creator of the work and the owner of the copyright in the work.²²⁵

²¹⁸ 17 U.S.C. §407 (2004) (effective November 13, 1997).

²¹⁹ 17 U.S.C. § 401(d) (2004), and *Original Appalachian Artworks v. The Toy Loft*, 684 F. 2d. 82, *supra* at 827.

²²⁰ 17 U.S.C. §302 (2004) (effective October 27, 1998).

²²¹ *Sony v. Connectix*, 203 F. 3d. 596, *supra*, note 212.

²²² 17 U.S.C. §102 (b) (2004).

²²³ 17 U.S.C. §102 (2004).

²²⁴ *Realization of Data Protection in Health Systems*, (1977) G. Griesser, (editor), at 3.

²²⁵ 17 U.S.C. §201(b) (2004).

f.) Policies on joint ownership and transfer of copyright should also be implemented in accord with statute.²²⁶ Note that under 17 U.S.C. section 202, ownership or transferred ownership of a copyrighted item does not necessarily mean that all of the copyrights are transferred as well. For example, one can own a piece of art but not have the right to reproduce the image.²²⁷

g.) Licensing agreements should be written with care. It is possible to put limits on what a licensee or a transferee can do relative to the copyrighted item.²²⁸

h.) And finally, it may be necessary, from time to time, to prosecute infringers. But, in each case, the possibility of winning a case, given the many defenses to infringement that are available, should be clearly evaluated.²²⁹

D. Protection of EMR Software through Trademark Law

1. Are Trademark Laws Applicable to EMR Software?

Another subsection of intellectual property law involves *trademarks* and *service marks*.

A *trademark* can be any kind of a word or symbol that acts to identify a product and its source and to distinguish it from other products that are or will be in the stream of commerce. It is sometimes referred to as a brand name. Likewise, a *service mark* provides the same distinction for a service.²³⁰

A *certification mark* is a type of marking, meant to avoid confusion in the market, and that indicates that a particular product or service comes from a certain area or is made by a certain group, (like the certification of a union label), or that the product or service

²²⁶ 17 U.S.C. §101 and U.S.C. §201(a)(2004).

²²⁷ 17 U.S.C. § 202 (2004).

²²⁸ 17 U.S.C. §201(d) (2004) and *Davidson v. Gateway*, 334 F. Supp. 2d. 1164 ,*supra*, note 216 at 1178.

²²⁹ *Gates v. Bando*, F. 3d. 823 (1993) *supra*, note 204, and 17 U.S.C. §107, and *Sony v. Connectix*, 203 F. 3d. 596,*supra*.note 212 (These provide examples of defenses to copyright infringement).

²³⁰U.S. Patent and Trademark Office, *What is a Trademark and a Service Mark?* (April 14, 2003) at <http://USPTO.gov> and 15 U.S.C. §1127 (2004) (effective March 29, 2000).

meets a certain standard of quality.²³¹ By statute, the owner of a certification mark cannot also make the product.²³²

For purposes of this writing, the laws dealing with trademarks, service marks and certification marks will hereinafter be referred to as trademark laws.

The rights conferred by trademark laws are different from other intellectual property rights in that a trademark right cannot exist by itself. The rights can only exist in connection with some type of commercial activity.²³³ Protections for trademarks began with state laws to guard against unfair competition and protections still exist at the state level.²³⁴ And so, actual first use in commerce of a trademark under the common law is enough to grant ownership of a trademark.²³⁵ But, the federal government eventually passed the Lanham Act²³⁶ as a type of national system of trademark registration and protection, obviously advantageous in an age of interstate commerce.²³⁷

Under the Lanham Act, the owner of a trademark can register for the exclusive use of a trademark²³⁸ The owner must certify in good faith that he is the correct user of the trademark²³⁹ and that the trademark is for use in commerce, whether currently or anticipated.²⁴⁰ A registration is generally good for ten years²⁴¹ and to rid the system marks that have not actually been used or where there have been problems, an affidavit is

²³¹ Miller, *supra*, note 61 at 240, 241, and 15 U.S.C. §1127(2004) (effective March 29, 2000).

²³² 15 U.S.C. §1064 (5) (2004) (effective August 5, 1999).

²³³ Miller, *supra* at 157, 158.

²³⁴ *Id.* at 159.

²³⁵ *Id.* at 228.

²³⁶ 15 U.S.C. §§1051 et seq (2004) (effective March 29, 2000).

²³⁷ Miller, *supra*, note 61 at 155 – 162.

²³⁸ 15 U.S.C. §1051 (2004) (effective March 29, 2000).

²³⁹ 15 U.S.C. §1051(a) (D) (2004) (effective March 29, 2000)..

²⁴⁰ 15 U.S.C. §1051(a) (C) (2004) (effective March 29, 2000)..

²⁴¹ 15 U.S.C. §1058 (2004) (effective November 2, 2002).

required to secure each ten year renewal period.²⁴² In theory, with continual use and re-registration, a trademark could last forever.

The national registration of a trademark affords three rights; the right to overcome any claims of later users of the mark, (publication of the mark gives constructive notice to others²⁴³), the right to sue for infringement in the federal courts and the right of incontestability.²⁴⁴ Incontestability means that if registration has been granted and in use for five consecutive years, not abandoned and verified as to use by affidavit within the sixth year; if the mark is not a generic name for some thing, a misdescriptive name, solely a geographic name, solely a functional name, an immoral name, or primarily merely the surname of a person; if the mark was not obtained fraudulently or with another owner's permission; if no final adverse decision regarding ownership of the right has been made and if there is no adverse proceeding pending, then, the registrant cannot be deprived of his registration.²⁴⁵ If the right is deemed incontestable, the registration is taken as evidence of validity of the mark and of its ownership rights.²⁴⁶ But, if the Patent and Trademark Office, (PTO), or a court finds proper cause as outlined above, that body can cancel a trademark.²⁴⁷

A trademark must be distinctive²⁴⁸ and a later user can contest the right to use a mark under the notion of priority of appropriation, unless the first user nationally registered

²⁴² 15 U.S.C. §1058 (b) (2004) (effective November 2, 2002) and 15 U.S.C. §1059 (a) (2004) (November 2, 2002).

²⁴³ 15 U.S.C. §1072 (2004).

²⁴⁴ Miller, *supra*, note 61 at 161 and 217-219,

²⁴⁵ 15 U.S.C. §1065 (2004) (effective March 29, 2000), 15 U.S.C. §1115 (2004) (effective November 2, 2002) and 15 U.S.C. §1052 (2004) (effective March 29, 2000).

²⁴⁶ 15 U.S.C. §1115 (b) (2004) (effective November 2, 2002).

²⁴⁷ 15 U.S.C. §1119 (2004).

²⁴⁸ 15 U.S.C. § 1052) (effective March 29, 2000).

first.²⁴⁹ A plaintiff can sue another for infringement of trademark rights if the competing mark or use of mark is likely to confuse the public.²⁵⁰ Such protests of infringement sometimes take the form of a complaint that the trademark's value is diminished or tarnished in some way.²⁵¹ Likelihood of confusion continues to be the greatest factor in determining if infringement exists.²⁵² In *Yale Electronic v. Robertson*, F. 2d 972 (1928), Judge Learned Hand likened a trademark to a reputation, remarking that, "[A] reputation, like a face, is the symbol of its possessor and creator; another can use it only as a mask."²⁵³ The party who uses a trademark first is usually, but not always, in a superior position to a party who uses a trademark second. A party who is a first user and has registered his trademark is definitely in a superior position relative to potential infringers or challenges to his trademark use.²⁵⁴

Recent court decisions involving the trademarking of computer software have dealt with traditional trademark issues as well as cyberpiracy concerns. In *Interstate Net Bank v. NETB@NK, inc.*, 221 F. Supp. 2d. 513 (2002), a federal district court ruled that the trademark name in question had become generic over time, allowing that an earlier registration of the mark was not incontestable because the definition of the original mark was more narrowly defined than the current practice.²⁵⁵

There is a provision in the Lanham Act forbidding cyberpiracy in misleading others in bad faith by using an internet domain name that can be confused with a trademark name.

²⁴⁹ 15 U.S.C. §1072 (2004), and Miller, *supra* at 165, 166.

²⁵⁰ Miller, *supra*, note 61 at 260.

²⁵¹ See *Sony Computer v. Connectix Corporation*, 203 F. 3d. 596, *supra*, note 212 at 608, 609.

²⁵² *Lambda Electronics v. Lambda Technology, inc.*, (1981) 515 F. Supp. 915 at 928.

²⁵³ *Yale Electric Corp. v. Robertson*, 26 F. 2d 972 (1928) at 974.

²⁵⁴ *Id.* at 928.

²⁵⁵ *Interstate Net Bank v. NETB@NK INC. and Netb@nk, CIVIL NO. 01-1324(JBS)* (2002), 221 F. Supp. 2d 513 at 522, 527.

²⁵⁶ The defendants in *Interstate Bank* countersued for cyberpiracy, maintaining that customers of online banking services were confused by two such similar domain names.²⁵⁷ But, knowing infringement, as required by the statute, was not found.²⁵⁸ In *S Industries v. Centra 2000*, 1998 WL 157067 (1998), the court looked at the likelihood that the public would be confused between two names on software, SENTRA and Centra. The test used by the court included asking if the marks were similar, not only in appearance but phonetically when evaluated as a unit; if the named products, the area and manner of use were similar; if consumers were experienced enough to use a high degree of care in choosing software of the type offered; if there was evidence of actual confusion and if there was evidence of actual intent to misappropriate the mark.²⁵⁹ In *Softman Products v. Adobe Systems*, 171 F. Supp. 2d. 1075 (2001), the court did not allow the defendant software company to succeed on counterclaims that a particular end user license agreement (EULA) could be used to limit a software distributor's legal right to distribute a product as he saw fit, especially if trademark confusion due to his distribution methodology was not proven.²⁶⁰

2. How can a Trademark on EMR Software be Protected?

a.) Before using or attempting to register a trademark, a good trademark search of competitors, in the U.S. and other countries should limit claims of infringement.²⁶¹

²⁵⁶ 15 U.S.C. §1125 (d) (2004) (effective November 29, 1999).

²⁵⁷ *Interstate Net Bank v. NETB@NK, INC.*, 221 F. Supp. 2d. 513, *supra*, note 255 at 513.

²⁵⁸ *Id.* at 527.

²⁵⁹ *S Industries, inc. v. Centra 2000, inc. et al*, No. 96 C 3524, 1998 WL 157067 (N.D. Ill.) ((1998) at 5,6.

²⁶⁰ *Softman Products Company, LLC v. Adobe Systems, Inc. et al*, No. CV 00-04161DDP (AJWX), 171 F. Supp. 2d 1075(2001) at 1083, 1093.

²⁶¹ Sellers, *supra*, note 11 at 100 and *Lambda v. Lambda*, 515 F. supp. 915, *supra*, note 252 at 920.

b.) Simply utilizing a trademark confers some protective benefit. Abandonment of a trademark is grounds for another to claim a right to use the mark and should be avoided.

262

c.) Registration should be completed. A U.S. registered trademark gives notice and provides evidence of ownership. It allows the owner to seek federal protection of his rights. Registration of a trademark, if filed with the U.S. Customs Service can be used to stop foreign importation of infringing products and as the groundwork for obtaining registration of the trademark in another country.²⁶³

E. Protection of EMR Software through Trade Secret Law

1. Are Trade Secret Laws applicable to EMR Software?

A *trade secret* is any information that is valuable to a business and is kept secret because of its competitive value.²⁶⁴ A trade secret could take many forms, including, but not limited to “a formula, pattern, compilation, program, device, method, technique, or process.”²⁶⁵ It has been held that as long as computer software can meet the criteria of trade secret, (a fact determinative inquiry), the software could also qualify as a form of information worthy of trade secret protections.²⁶⁶

Federal law provides some measure of protection of trade secrets in its criminal code against economic espionage.²⁶⁷ These codes have a heavy emphasis on protecting American commerce from unlawful foreign infiltration.²⁶⁸ But, trade secret law is generally the law of the states, involving some combination of the laws of torts, property

²⁶² 35 U.S.C. §1115 (b) (2) (2004) (effective November 2, 2002).

²⁶³ U.S. Patent and Trademark Office, *What are the Benefits of a Federal Trademark Registration?* (April 14, 2003) at <http://USPTO.gov>.

²⁶⁴ Uniform Trade Secrets Acts §1 (4) (i),(ii)(2004).

²⁶⁵ Uniform Trade Secrets Acts §1 (4)(2004).

²⁶⁶ *Amoco Production Company v. Lindley*, No. 51543, 609 P. 2d. 733 (1980) at 744, 743.

²⁶⁷ 18 U.S.C. §1831 et seq (2002).

²⁶⁸ *Id.*

²⁶⁹ and contracts. ²⁷⁰ Trade secret law can provide some protections for matter which would not necessarily meet the rigorous requirements set out under federal patent law. ²⁷¹ Currently, 45 states have adopted versions of the Uniform Trade Secrets Act, (UTSA), ²⁷² which is a manifestation of an early restatement of the law of torts. ²⁷³ The Restatement of Torts contains six factors that must be considered when determining if something is a trade secret. They are 1) the extent to which people outside of the business, 2) and the extent to which people inside the business know about the secret, 3) the nature of security measures taken to guard the secret, 4) the value of the secret information, 5) the expense of developing the secret, and 6) the effort that would be necessary to copy the secret. ²⁷⁴ Use of state laws to protect trade secrets often hinges on an analysis of whether a trade secret does indeed exist. ²⁷⁵

Trade secrets may also sometimes consist of patentable subject matter, enabling protection under two areas of the law. ²⁷⁶ Although, in general, it is thought that patent protection provides a superior safeguard to trade secret protection. ²⁷⁷

The protections of trade secret law are most effective at the developmental stage, before a product has been marketed and the threat of reverse engineering becomes real. During this period, patentability will still be an uncertain prospect, and to a certain extent, the protection offered by trade secret law may “dovetail” with the incentives created by the federal patent monopoly.²⁷⁸

²⁶⁹ *Bonito Boats, inc. v. Thunder Craft Boats, inc.*, No. 87-1346, 489 U.S. 141 (1989), at 157.

²⁷⁰ *Kewanee Oil v. Bicron* 416 U.S. 470 *supra*, note 145 at 486, 487 and *Amoco v. Lindley*, 609 P. 733, *supra* at 736.

²⁷¹ *Kewanee Oil v. Bicron*, 416 U.S. 470, *supra*, note 145 at 482.

²⁷² ULA Trade Sec Refs & Annos, at Table of Jurisdictions Wherein Act has been Adopted.

²⁷³ Restatement (First) of Torts (1939) §757 and *Kewanee Oil Company v. Bicron Corporation et al*, No. 73-187, 416 U.S. 470 (1974) at 474, 475.

²⁷⁴ Restatement (First) of Torts (1939) §757 cmt. b.

²⁷⁵ Restatement (First) of Torts (1939) §757, *supra* at cmt. b and *Amoco v. Lindley*, 609 P. 2d 733, *supra* note 266 at 747.

²⁷⁶ *Kewanee Oil v. Bicron*, *supra*, 416 U.S. 470, *supra*, note 145 at 487, 488.

²⁷⁷ *Kewanee Oil v. Bicron*, *supra*, 416 U.S. 470, *supra*, note 145 at 488.

²⁷⁸ Chisum, et al, *supra*, note 60 at 1191.

State law that regulates the intellectual property in trade secrets cannot conflict with federal law, i.e. the law of copyrights and patents, as the federal law operates under a Constitutional mandate to regulate commerce and ‘to promote the Progress of Science and the Useful Arts’.²⁷⁹ The court in *Kewanee Oil Co. v. Bicron corp. et al*, 416 U.S. 470 (1974), noted that state trade secret law and federal patent law can potentially co-exist in instances whereby trade secret law can protect items of “lesser or different invention”, but still important to technological progress.²⁸⁰ But, a state law that allows a monopoly in contravention of the objectives of federal intellectual property law cannot stand and will be preempted by the Supremacy clause of the U.S. Constitution.²⁸¹ The failure to receive a patent for an invention does not necessarily preclude protections that exist in a contract pursuant to a state trade secret law.²⁸² Under certain conditions, inventors can use both kinds of protections successfully.²⁸³ But, “a trade secret does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering...”.²⁸⁴ With a trade secret, there is a high risk that the secret will be discovered by accident or by deliberate means and that the source of the breach may not be easily discoverable.²⁸⁵

Conflicts relative to trade secrets often arise during negotiations of *ownership* and *use* of the secret.²⁸⁶ With agreements concerning computer software, holders of a trade secret

²⁷⁹ *Kewanee Oil v. Bicron*, 416 U.S. 470, *supra*, note 145 at 479, 480 and U.S. Const. Art. I, sec. 8, cl.3, cl. 8.

²⁸⁰ *Kewanee Oil v. Bicron*, 416 U.S. 470, *supra*, note 145 at 493.

²⁸¹ *Bonito Boats v. Thunder Craft Boats*, 489 U.S. 141, *supra*, note 269 at 156, 157 and 168.

²⁸² *Jane Aronson v. Quick Point Pencil Company, No. 77-1413*, 440 U.S. 257 (1979) at 257.

²⁸³ *Id.* at 358.

²⁸⁴ *Kewanee Oil v. Bicron*, 416 U.S. 470, *supra* note 145 at 476.

²⁸⁵ *Id.* at 490.

²⁸⁶ For example, see *S.O.S., inc., v. PAYDAY, inc., Nos. 88-5817, 88-5878*, 886 F. 2d. 1081 (1989) at 1083 and 1084.

may allow use of the software while at the same time blocking access to the object code, (that part of the program not readily understandable by the programmer).²⁸⁷ Such licensing agreements as well as employment agreements and other contracts are often offered as evidence and hotly contested when courts try to determine if a defendant misappropriated the trade secret or used fair means to acquire the secret.²⁸⁸

Regarding computer software, charges of copyright violations as well as trade secret violations are often made together.²⁸⁹ In *Computer Associates International v. Altai*, 982 F. 2d. 693 (1992), a federal court held that as long as state trade secret law is applied to a case such that the domains of trade secret and of copyright can be distinctly defined, the federal copyright law would not preempt the state cause of action on a claim of software espionage.²⁹⁰

2. How can a Trade Secret Relative to EMR Software be Protected?

The Uniform Trade Secret Act (UTSA) very clearly defines trade secret, misappropriation of trade secret and the circumstances under which there is a duty to keep a trade secret.²⁹¹

a.) It is important to differentiate between trade secret information and general knowledge. The universal skills or subjective information learned by an employee on the job that are not trade secrets are generally not protected by the UTSA.²⁹²

²⁸⁷ *S.O.S v. PAYDAY*, 886 F. 2d. 1081, *supra*, note 286 at 1090.

²⁸⁸ For example, see *S.O.S v. PAYDAY*, 886 F. 2d. 1081, *supra*, note 286, and *Amoco v. Lindley*, 609 P. 2d 733, *supra*, note 266 and *Aronson v. Quick Point Pencil*, 440 U.S. 257, *supra*, note 282 and *Sperry Rand Corporation v. Pentronix, inc.*, *Civ. A. No 43109*, 311 F. Supp. 910 (1970), and *Evolution, inc. v. Suntrust Bank, et al*, *No. CIV. A. 01-2409-CM*, F. Supp. 2d. (2004).

²⁸⁹ For example, see *S.O.S v. PAYDAY*, 886 F. 2d. 1081, *supra*, note 286 and *Computer Associates International, inc. v. Altai, inc.*, *No. 762, Dockets 91-7893, 91-7935*, 982 F. 2d 693 (1992).

²⁹⁰ *Computer Associates International, inc. v. Altai, inc.*, 982 F. 2d 693, *supra*, note 289 at 721.

²⁹¹ Uniform Trade Secrets Act §1 (4), (2), (II) and (III) (2004).

²⁹² 42 Am. Jur. 2d Injunctions §133.

b.)The lengths to which an employer must go in keeping a trade secret confidential under UTSA are not as clear.²⁹³ Nevertheless, within those states using the UTSA as the format for their trade secret laws, it is critically important for organizations expecting to be able to prosecute for misappropriation of trade secrets to take precautions that are reasonable under the circumstances to guard those secrets.²⁹⁴ It is generally accepted that while employed and at termination of employment, an employee is expected not to disclose his employer's confidential information, including trade secrets. This concept has been upheld in the courts in circumstances with and sometimes without express notations in employment agreements.²⁹⁵ In any case, privacy agreements between employers and employees, contractors and licensees are recommended.²⁹⁶ A reasonable agreement between an employer and an employee or contractor or licensee in which there is an condition not to reveal confidential information like trade secrets is usually enforceable in the courts.²⁹⁷ Conversely, courts may find agreements unreasonable and therefore unenforceable if the agreement goes beyond protecting employer interests and restricts free trade.²⁹⁸ In *Computer Print Systems v. David A. Lewis*, 281 Pa. Super 240 (1980), a state appeals court deemed that an executive's assertion that computer programs were to remain "in house" and his expectations that his employees would accordingly not reveal secret computer program information was enough to afford trade secret protection to that software.²⁹⁹ But in *Computer Associates v. Altai*, an appeals court found the fact that a

²⁹³ Uniform Trade Secrets Act §1(4)(ii) (2004).

²⁹⁴ *Id.*

²⁹⁵ 42 Am Jur. 2d Injunctions §131 citing 27 Am Jur. Employment Relationship §224.

²⁹⁶ See examples of agreements in 7B Am. Jur. Legal Forms 2d Employment Contracts §99:195.

²⁹⁷ *Julius Hyman & Co et al v. Velsicol Corp., No. 16084*, 233 P. 2d 977 (1951) at 621 and 27 Am. Jur. 2d Employment Relationship § 179.

²⁹⁸ *State Medical Oxygen and Supply, inc. v. American Medical Oxygen Co.*, 240 Mont. 70 (1989) at 75 and 27 Am. Jur. 2d Employment Relationship § 179.

²⁹⁹ *Computer Print Systems v. David A. Lewis*, 281 Pa. Super. 240 (1980) at 253.

computer company executive who hired a friend, ostensibly not knowing that the friend has brought with him to his new job purloined computer software from his last employer, to be the subject of a remand for determination of whether the hiring executive should have constructively known of the theft. Such constructive knowledge can make the new employer and his company vicariously liable for damages as a result of misuse of the secret.³⁰⁰

A company policy that employees must sign a confidentiality agreement, was enough to help guarantee that a customer list in question would be considered worthy of trade secret protection in *American Credit Indemnity Co. v. Lola N. Sacks*, 213 Cal. App. 3d. 622 (1989), even though the accused employee claimed never to have signed the agreement.³⁰¹

Yet, when a plaintiff demonstrated a mechanical improvement to a Yamaha motorcycle to the cycle's manufacturer who later marketed the same improvement, the plaintiff was not permitted by the court to claim trade secret protection, as he had freely shared his knowledge with no restriction.³⁰²

c.) Especially with EMR software where confidential patient information may be involved, heightened security arrangements beyond the employee/contractor/licensee privacy agreement should be implemented. Such precautions could include secured storage of physical products and destruction of no longer needed products³⁰³, computer passwords, audit trails, enabling technology and encryptions³⁰⁴, as well as specialized monitoring and anti-virus protections.³⁰⁵

³⁰⁰ *Computer Associates International v. Altai, Inc.*, 982 F. 2d 693, *supra*, note 290 at 719.

³⁰¹ *American Credit Indemnity Co. v. Lola N. Sacks*, No. B034560, 213 Cal. App. 3d 622 (1989) at 631.

³⁰² *Wilbert J. Sheets v. Yamaha Motors, Corp. U.S.A. et al*, No. 87-3420, 849 F. 2d 179 (1988) at 182, 183.

³⁰³ Joseph Goedert, *Newsline: Store, Burn or Shred: What to do with Paper Records?*, Health Data Management, February 2, 2004, vol. 12, no. 2, 2/2/04 HDAMGMT 18 at [2004 WL 62524484](#) at 1,2.

³⁰⁴ Siwicki, *supra*, note 44 at 7.

³⁰⁵ Morrissey, *supra*, note 33 at 1.

d.) Policies and procedures mandating security arrangements and confidentiality agreements, working in tandem with emerging technologies, are always valuable.³⁰⁶

V. Mentoring and Protecting Intellectual Property within the EMR Software

Development Process

Capitalizing on the best value of intellectual property involves the coordination of strategy, policy, education, incentives and enforcement. Management, employees, contractors, consultants³⁰⁷ and vendors are all a part of the process. (See IV. B. 2., C. 2., D. 2., E. 2., *supra*). To mentor toward a positive outcome, an organization may consider the following actions.

A. Conduct an internal inventory to capture IP that already exists or to identify areas where IP may grow.³⁰⁸ Sometimes opportunities for IP exist in departments that do not traditionally invent, like the marketing department that is creating a brand.³⁰⁹ Once a feel for existing IP is available, a baseline for record keeping will exist and an analysis of the relative value to the organization of each existing creation can be completed.³¹⁰

B. Then, wherever desirable and possible, ownership of the IP through the appropriate means should be asserted. Decisions should be deliberate. For example, a trademark registration should not be allowed to lapse unless that is an organizational decision,³¹¹ patents should be prosecuted according to statute³¹², a notice of copyright published.³¹³

³⁰⁶ *Technology is Changing the Health Data Security Landscape, Health Data Management*, September 19, 1997, 9/19/97 HDAMGMT (pg. unavail. Online) at [1997 WL 8747994](#) at 2.

³⁰⁷ Carter, *supra*, note 6 at 109.

³⁰⁸ Sellers, *supra*, note 11 at 82,101.

³⁰⁹ *Id.* at 81,82.

³¹⁰ *Id.* at 88.

³¹¹ 15 U.S.C. §1115 (2004) (effective November 2, 2002).

³¹² 35 U.S.C. §§101 (2004). §102 (2004) (effective November 2, 2002), §103 (2004) (effective November 29, 1999).

³¹³ 17 U.S.C. §401(d) (2004).

and trade secret confidentiality agreements implemented³¹⁴. Disclosure and assignment agreements should be signed and ownership through contracts and license agreements clarified. (See IV. B. 2., C. 2., D. 2., E. 2., *supra*.) For government funded research, the mandates of the Bayh-Dole Act relative to patents for inventions created should be seriously followed.³¹⁵ Rights acquired through IP ownership should be exercised.³¹⁶

C. Implement a system of external research.³¹⁷ Note what competitors are doing so that liability for infringement can be limited. External research can be used to aid decision making about what IP should be divested or purchased for to benefit the organization's portfolio.³¹⁸ For example, perhaps a no longer useful trademark could be sold, a piece of software licensed, or a patent purchased.³¹⁹ Software, accessed through websites like that offered by the PTO can be used to monitor software developments and to continue to gain education on intellectual property.³²⁰ Many computer *blogs*, (online journals)³²¹, exist that are helpful in tracking intellectual property developments.³²²

D. Create and implement a series of policies, guidelines, procedures, and agreements relative to disclosure, employment, (especially work-for-hire agreements), incentives, licensing, contracting and applying to intellectual property protections and EMR safety,

³¹⁴ *Julius Hyman v. Velsicol*, 233 P. 2d. 977 *supra*, note 297 at 621.

³¹⁵ 35 U.S.C. §§200 et seq. (2004) (Effective November 1, 2000).

³¹⁶ Syrowiak, *supra*, note 105 at 5.

³¹⁷ Sellers, *supra*, note 11 at 101 and *Intellectual Property*, (2004) at <http://FindLaw.com>.

³¹⁸ Sellers, *supra*, note 11 at 101.

³¹⁹ *Id.*

³²⁰ *Id.* at 100.

³²¹ Todd Chatman, *Join the Blog Bandwagon*, ABA Student Lawyer, vol. 33, no. 4 (December, 2004) at 19.

³²² Dan Harmon, *LOA-Office Automation : Computer Hardware & Software*, Lawyer's PC, December 1, 2004, at [22 No. 5 LAWPC 15](#) at 2, citing Robert Ambogi, *Web Watch*, Law Technology News, October 2004, at 52.

security and integrity.³²³ (And, see IV. B. 2., C. 2., D. 2., E. 2., *supra*). Compliance with policies should be monitored.³²⁴

E. Educate all concerned, especially managers and employees, about intellectual property, EMR safety, security and integrity, and the part that they play in successful strategy.³²⁵

F. Heighten security surrounding the EMR and EMR software development.³²⁶

G. Avoid unnecessary litigation costs by not infringing on the intellectual property rights of others and prosecute infringement to the point where it is in line with organizational strategy.³²⁷ (And, see IV. B. 2., C. 2., D. 2., E. 2., *supra*).

VI. Conclusion

The intellectual property in EMR software and its development can be protected using a variety of laws, good management and organization-wide education. For a positive outcome, the process must be strategic and pervasive.³²⁸ When managers and other employees of the healthcare system understand the part that they play in maintaining the legal integrity of the EMR software development process, the organization and its patients will benefit.

³²³ Computer Science and Telecommunications Board of the National Research Council, For the Record: Protecting Electronic Health Information, (1997) at 127-142.

³²⁴ Sellers, *supra*, note 11 at 101.

³²⁵ Sellers, *supra*, note 11 at 101 and Computer Science and Telecommunications Board of the National Research Council, *supra*, note 323 at 142-149.

³²⁶ Realization of Data Protection in Health Systems, *supra*, note 224 at 3 and Goedert, *supra*, note 303 at 1, 2 and Institute of Medicine, *supra*, note 9 at 214, 217.

³²⁷ Sellers, *supra*, note 11 at 101.

³²⁸ Robert R. Lech, *Protecting Computer Software Against Reverse Engineering*, Michigan Law Journal, June, 1994, 73 Mich. B.J. 626 at 4.

