Using the DNA Profile as the Unique Patient Identifier in the Community Health Information Network: Legal Implications, 15 J. Marshall J. Computer & Info. L. 227 (1997)

Lisa L. Dahm
USING THE DNA PROFILE AS THE UNIQUE PATIENT IDENTIFIER IN THE COMMUNITY HEALTH INFORMATION NETWORK: LEGAL IMPLICATIONS

by Lisa L. Dahm†

An invasion of armies can be resisted, but not an idea whose time has come.

— Victor Hugo, Histoire d'un Crime [written 1852], conclusion

Maoir ignotarum rerum est terror. (Apprehensions are greater in proportion as things are unknown.)

— Livy, History, Bk. xxviii, sec. 44 (c. 10 B.C.)

TABLE OF CONTENTS

I. INTRODUCTION ....................................... 228
II. BACKGROUND ......................................... 233
   A. The DNA Profile .................................. 233
   B. Generating the Unique DNA Fingerprint — RFLP Analysis ................................. 234
   C. DNA Profiling is Accepted by the Scientific Community ................................... 236
III. USE OF DNA FINGERPRINTS IN THE HEALTHCARE DELIVERY SYSTEM IS TIMELY ...... 238
   A. Sharing Information Between and Among Providers is Essential .......................... 239
   B. No Standard Identifier Currently Exists ......................................................... 242
IV. ANALYSIS ........................................... 246

† Copyright © 1997 by Lisa L. Dahm. All rights reserved. The Author is a recognized expert in the healthcare information systems (“HCIS”) industry with over twenty years of experience in sales, marketing, support services, installations, planning documentation, and education. She graduated with honors from South Texas College of Law in Houston, Texas and is currently the Associate Corporate Counsel for a large non-profit hospital system in the same city.
A. PERCEIVED CHALLENGES AND OBSTACLES BARRING USE OF THE DNA FINGERPRINT AS A UNIQUE PATIENT IDENTIFIER ........................................... 246

B. VALIDITY OF THE DNA FINGERPRINTING PROCESS ....... 246
   1. Current Misconceptions About the Process and the Outcomes ........ 247
   2. Costs in Time and Labor Associated with the Process ....................... 250

C. OWNERSHIP AND SECURITY OF AN INDIVIDUAL'S DNA FINGERPRINT ....................................... 251
   1. Producing a Specimen for DNA Testing ........ 251
   2. The Concept of Informational Privacy ........ 254
   3. Ownership and Control of DNA Fingerprint Databases ....................... 258
   4. Maintaining DNA Information in the Healthcare Industry ................. 262
   5. Protections Against Unauthorized Disclosure of Sensitive Medical Data Exist ........ 266

V. CONCLUSION: IMPLEMENTING THE PROPOSAL... 272

I. INTRODUCTION

Like the weather, the healthcare industry changes constantly and rapidly. Currently, two distinctly different trends receive the majority of attention from those within and outside of the industry: (1) development and implementation of clinical information systems to improve the quality of patient care, specifically Clinical Data Repositories ("CDR")1 or the electronic medical record;2 and, (2) mergers and acquisitions within the

1. John Morrissey, Automated Patient Record In Spotlight, MOD. HEALTHCARE, June 19, 1995, at 142 (predicting that the automated patient record will become the dominant healthcare information systems offering within five years). A consulting report published by R.L. Johnson & Associates predicts that sales of clinical data repositories and the necessary connectivity hardware and software will reach $1 billion by 1999. Id.

The automated patient medical record is just one of the components in a CDR. Other components include personal computer-based physician workstations, the relational database necessary for the storage of the information, an interface engine used to capture data from clinical systems, and optical or magnetic disk for storing active and long-term patient records. R.L. Johnson, CDRs: More Hype Than Help?, 6 NO. 6 HIMSS NEWS, June 1995, at 10.

2. For the purposes of this article, an "electronic medical record" is one that is maintained either wholly or partially on an information system used by the healthcare facility. The medical record includes personal, financial, social, and clinical information about the individual patient. ROACH ET AL., MEDICAL RECORDS AND THE LAW 1 (Aspen Systems Corp. 1985). See also Terri F. Arnold, Note, Let Technology Counteract Technology: Protecting The Medical Record In The Computer Age, 15 HASTINGS COMM. & ENT. L.J. 455, 455 (1993). The medical record documents the care given to the patient, providing a chronological assessment of the treatment plan and its execution. ROACH, supra, at 2. Keeping a
industry, resulting in smaller numbers of bigger healthcare providers and facilities.³

At first glance, little overlap appears to exist between the first and second trend. A single healthcare provider⁴ can plan for, evaluate, select, and finally implement either a CDR or an electronic medical record with little or no involvement from others in the healthcare industry. However, the individual provider that ignores the effect of the second trend, while devoting time and attention to the first, risks wasting enormous amounts of time and money.⁵ Despite Congressional defeat of the Health Security Act in 1994, healthcare reform continues.⁶ If nothing

medical record on each patient is required by law, but also allows healthcare providers to provide better patient care and to minimize malpractice losses. JONATHAN P. TOMES, HEALTHCARE RECORDS: A PRACTICAL LEGAL GUIDE 67 (HFMA, Kendall/Hunt Publ'g Co. 1990). “Some states define the term medical record, and others merely specify what information such a record must contain.” Id. at 3. Although comprehensive review of the components of the medical record by state is beyond the scope of this article, Mr. Tomes provides such detail in his book. Id. at 4-65. For standards of medical records required for healthcare facility accreditation, see generally American Hospital Association and The Joint Commission on Accreditation of Healthcare Organizations, The Joint Commission's 1994 Accreditation Manual For Hospitals: Management Of Information And The Indicator Management System, Nov. 11, 1993, at 377-435.


4. For purposes of this article, a “healthcare provider” is any single organization that renders services to individual patients: a hospital; a physician’s office; a long-term care facility; an ambulatory care center; a clinic; or a managed care organization that renders services to individual patients. The provider organization can be relatively small, like a solo physician practitioner, or relatively large, such as a 1500-bed tertiary hospital. A healthcare entity is comprised of one or more healthcare providers or a combination of any of the provider types.

5. “Health care providers are beginning to appreciate the value of sharing information to be more efficient, and thus more competitive.” Françoise Gilbert, Selected Legal Issues In The Use Of Community Health Information Networks, 9 No. 2 J. HEALTHCARE INFO. & MGMT. SYSTEMS SOC’Y 9, 43 (1995).

else, consumers, providers, payors, and vendors recognize and acknowledge that costs associated with sharing information rather than duplicating it, time after time, are significantly less. A shared data base containing comprehensive financial and clinical information accessible to those in the sharing group, regardless of location, may decrease and, in some cases, eliminate errors of communication or transmission of the information. Newly merged and acquired providers and entities usually encounter information that is totally or partially inaccessible as a result of disparate information systems installed in their predecessor organizations—“islands of information” that must be incorporated and absorbed into the new information system architecture. Indeed, even providers that remain independent and autonomous have a similar need to share information across the industry.

Incorporating or simply sharing information between providers or entities, however, is not as easy as it sounds. Within a single provider or entity, different types of providers render different types of care. More importantly, each provider or subgroup within a provider or entity may use different computers to run different software programs that provide management reports identifying different problems and results. One of the biggest obstacles to sharing information between entities or incorporating information from diverse systems within a newly merged provider organization is the lack of a single, unique patient identifier. Each individual healthcare provider and system has its own way of identifying “its” patients. When information is prepared by one provider or system

---


9. A variety of identifiers are currently in use by different systems. Some information systems use an encounter-based numbering scheme, whereby the patient receives a base number, which identifies the patient's financial or medical record number, combined with a three- or four-digit suffix, which represents the number of times that individual receives
in response to a request from another provider, entity, consumer, or legal office, there is always a risk that the wrong patient's information will be transferred. Provider departments that complete tests without ever seeing the patient may receive specimens labeled by patient name, financial account number, or medical record number, instead of the department's unique patient identifier. If providers use the patient's initials rather than the patient's full name, specimens from patients with the same first initial and surname may be mislabelled and have to be repeated for the appropriate patient. Similarly, transposing one or more numbers in a financial account number can cause discrepancies in patient insurance bills and statements, which is a major source of patient and provider frustration.

This article proposes using each individual's unique deoxyribonucleic acid ("DNA") fingerprint as his/her personal patient identifier, regardless of which provider or entity renders healthcare services. This article also addresses the legal issues concomitant with implementing this proposal. By using DNA profiles as unique patient identifiers, this author believes that the major goals of each industry trend can be achieved simultaneously. First, a single patient medical record, which is the foundational requirement for a successful CDR or electronic medical record, promotes efficiency and improved patient care, two of the articulated benefits that can be realized from implementing a CDR or an electronic medical record system. In organizations that plan to implement, or have implemented, a CDR or an electronic medical record system,10 services at the facility. Other information systems use multiple numbers for each patient, one for financial records and one for clinical records. These systems usually include cross-reference capabilities so that employees who have access to a patient's financial record can see the clinical record number and vice versa. In relatively sophisticated systems of this type, however, access to the financial records by a clinician or access to the clinical records by a financial employee is prohibited. Still other systems use one number to access both types of records. In many cases, this number is randomly generated, or it may even be the patient's social security number.

The social security number is no longer used solely as a "social security number." See Minor, supra note 8, at 263 (quoting the Report to the Commissioner by the Social Security Number Task Force). In 1974, Congress passed the Privacy Act of 1974 in an attempt to restrict governmental use of the social security number, but the Tax Reform Act of 1976, passed only two years later, "authorized the states to use the [social security number] for a wide range of purposes." Id. at 264-65. Unfortunately, since use of the social security number is so widespread, once an entity possesses an individual's social security number, a wealth of information is accessible on that individual. Id. at 266. See infra notes 65-76 and accompanying text.

10. In a recent survey conducted jointly by the Healthcare Information and Management Systems Society ("HIMSS") and Hewlett-Packard, only six percent of the 976 respondents indicated that they have no plans to computerize their patient records. Nancy Aldrich & Richard Corley, Information Systems Professionals Cite Trends In Healthcare Computing, HEALTHCARE INFORMATICS, May 1995, Special Report, at 18. Twenty-four per-
each patient is assigned a unique number that does not change, regardless of the number of encounters with the facility; applying the proposal, the patient's unique number would be a bar code representation of the patient's DNA fingerprint. Therefore, any given patient's record will contain all pertinent health data from every encounter that patient has with that facility from birth to death. Similarly, where mergers and acquisitions have resulted in a single larger entity with numerous but disparate financial and clinical systems, a unique patient identifier—the DNA fingerprint—will be standard regardless of which financial or clinical system is used. Having one unique patient identifier will eliminate at least one interface requirement and facilitate sharing of information within the entity and across the healthcare industry.

Part One of this article presents a brief overview of the DNA profile, specifically, how the profile is generated, and its current status in the scientific community. Part Two explores the shift to Community Health Information Networks ("CHIN")\textsuperscript{11} and Integrated Delivery Systems ("IDS")\textsuperscript{12} in order to establish the timeliness of this proposal. Part Three reviews major misconceptions about the DNA profile shared by members of the legal community and the public at-large. This section also explores the ramifications associated with using the DNA profile as the unique identifier, including validity of the DNA profiling process, issues of ownership and security of information, individual privacy concerns, and current and proposed pertinent legislation. Finally, Part Four

\textsuperscript{11} A CHIN is "an integrated collection of computer and telecommunications capabilities that facilitate communications of patient, clinical and payment information among multiple providers, payors, employers and related healthcare entities within a community." Kathleen Frawley, \textit{Achieving The CPR While Keeping An Ancient Oath}, HEALTHCARE INFORMATICS, April 1995, at 28; see also infra notes 54-64 and accompanying text (discussing concurrent focus on information sharing and information security, and their relationship to success of CHIN).

\textsuperscript{12} An IDS is a group of different healthcare providers operating together to deliver health care services. Lisa S. Paul, \textit{IDS vs. CHIN: The Great Debate?}, INFOCARE, May 1995, at 42, 44. According to one industry consultant, the difference between a CHIN and an IDS is that groups work together within an IDS whereas they compete within a CHIN. \textit{Id.} at 42

IDSs have developed in response to the economic pressures of managed care and usually are formed by a prime provider such as a hospital or medical center. The prime provider subcontracts with physician practices and other allied health facilities to deliver cradle-to-grave services to a population covered by a managed care insurance plan.

Cassie Dillon, \textit{Building An Information Bridge For Integrated Delivery Systems}, HEALTHCARE INFORMATICS, July 1995, at 24. More than seventy percent of the HIMSS—Hewlett Packard survey respondents are forming or planning an IDS. Aldrich & Corley, supra note 10, at 18; see infra notes 54-55 and accompanying text (discussing importance of information sharing to success of CHIN and IDS).
presents an action plan for adopting the proposal and its associated costs and benefits.

II. BACKGROUND

A. THE DNA PROFILE

In 1953, James Watson and Francis Crick discovered the double helical structure of deoxyribonucleic acid, or DNA. DNA is the material of which chromosomes are made; the chromosomes in each cell comprise the “blueprint” for a human body. Each chromosome contains the four nucleotide bases, adenine, thymine, cytosine, and guanine, that always pair in the same distinct patterns; adenine always pairs with thymine, and cytosine with guanine. Yet surprisingly, with the exception of identical twins, no two people have the same DNA. A particular sequence of base pairs is a gene, and each human cell contains between


14. Dan L. Burk, DNA Identification Testing: Assessing The Threat To Privacy, 24 U. TOL. L. REV. 87, 89 (1992) [hereinafter Burk Testing]; Lisa B. Hansen, Comment, Stemming The DNA Tide: A Case For Quality Control Guidelines, 16 HAMLIN L. REV. 211, 214 (1992); K.F. Kelley et al., Method And Applications Of DNA Fingerprinting: A Guide For The Non-Scientist, CRIM. L. REV. 105, 105 (1987). DNA is present in the nucleus of every cell. In order to extract DNA, therefore, a specimen comprised of cells with a nucleus, such as blood, bones, skin, or even cells from scraping the inside of the mouth must be gathered. Interview with Sara Bowne, Assistant Toxicologist and DNA Analyst at the Medical Examiner’s Office of Houston, Texas (June 13, 1995) [hereinafter Bowne Interview]. However, because red blood cells contain no nucleus, it is the white blood cells from the blood sample that are used to extract DNA. Id. See also Michael J. DiRusso, Note, DNA “Profiles”—The Problems Of Technology Transfer, 8 N.Y.L. SCH. J. HUM. RTS. 183, 183 (1990); Hoeffel, supra note 13, at 469. Note that samples other than blood might be required from people who have an immune deficiency diseases since those diseases may result in either a minimal number of or no white blood cells. Bowne Interview, supra.

15. Hoeffel, supra note 13, at 470. See also JoAnn M. Longobardi, Note, DNA Fingerprinting And The Need For A National Data Base, 17 FORDHAM URB. L.J. 323, 326-27 (1989). Each DNA molecule is a double helix that, unraveled, would be approximately six feet long. Hoeffel, supra note 13, at 469; Captain Huber, Battling Chromosomes: Fighting “DNA Fingerprinting” Evidence, 1993 JUN ARMY L. 38, 38 (1993). Each double helix is a twisted ladder of sugars and phosphates “with pairs of nucleotide bases (base pairs) forming the rungs of the ladder.” Id. Although there are approximately 3.3 billion base pairs in each DNA molecule, only four bases adenine exist—(A), thymine (T), cytosine (C), and guanine (G). Hoeffel, supra note 13, at 469; Huber, supra, at 38; Christine K. Cassel & Dana Levinson, The Human Genome Project: Who’s Looking Out For ELSI?, HOSP. PRAC., April 15, 1995, at 11.

60,000 and 80,000 genes. Genes determine each individual’s unique traits—hair or eye color, height, pre-disposition to disease, and so forth. Many people have blue eyes, and the gene that determines blue eyes is located at approximately the same place on the same chromosome in every blue-eyed person. Nonetheless, the base pairs that comprise the gene in one individual usually differ significantly from the gene for blue eyes in a different individual. These areas of genetic variation are known as “polymorphisms,” the areas targeted for DNA profiling.

B. Generating the Unique DNA Fingerprint—RFLP Analysis

In 1984, Alex Jeffreys, a British geneticist, “devised a way to visually identify DNA found between the genes.” His method is called re-

17. Hoeffel, supra note 13, at 470; Carey, supra note 13, at 74.
18. Snyder, supra note 16, at 204-05; Burk Testing, supra note 14, at 89; Hoeffel, supra note 13, at 470.
21. Huber, supra note 15, at 38 (describing alleles and DNA profiling). See also Snyder, supra note 16, at 205; J. Clay Smith, Jr., The Precarious Implications Of DNA Profiling, 55 U. PIT. L. REV. 865, 869 (1994); Hoeffel, supra note 13, at 470-71; Robert A. Hegel, M.D., Molecular Forensics: Applications, Implications And Limitations, 141 CMAJ 668, 668 (1989). Traditionally, polymorphic forms of the ABO blood grouping and the human leukocyte antigen have been the basis for serologic typing and forensic identification of individuals. Hegel, supra, at 669. Today, instead of the 90 to 95 percent certainty of traditional blood group and antigen testing, DNA profiling, or fingerprinting, can identify an individual with “virtual certainty.” Debra C. Moss, Evidence, DNA—The New Fingerprints, 74-May A.B.A. J. 66, 68 (1988). See also ABC News Primetime Live: Beyond A Reasonable Doubt (ABC television broadcast, Feb. 4, 1993) (reporting that DNA testing has become a powerful new tool in fighting crime in the last five years).

In 1983, a teenage girl was sexually assaulted and murdered near the English village of Enderby. Sharon Begley, Leaving Holmes In The Dust, Newsweek, Oct. 26, 1986, at 81. Two years later, another teenage girl was assaulted and murdered in virtually the same location. Id. Although the police had arrested no one in connection with the first girl’s murder, they did have semen samples taken from both victims. Id. After the second murder, they requested “4,000 local men to voluntarily submit a blood sample from which the crime lab could take ‘DNA fingerprints’—in effect, partial maps of a human gene” in hopes of finding a match between a blood DNA print and the semen DNA prints. Id. When Colin Pitchfork tried to have a friend take his place for the blood test, police arrested and formally accused him of both murders. Id. “[F]or the first time the new forensic technique of
DNA AS A UNIQUE PATIENT IDENTIFIER

Restriction fragment length polymorphism ("RFLP") analysis. In RFLP analysis, DNA is first extracted and purified from human tissue, blood, or other human bodily fluid containing nucleated cells. The purified DNA is then cut into fragments using enzymes that recognize certain sequences in nucleotide bases. Next, the resulting fragments are sorted by length, they are split, and then they are transferred to a nylon sheet. After immersing the sheet containing the fragments in a bath, radioactive probes, which are DNA segments of known sequence that bond to specific base sequences, are added to the bath. Finally, the sheet is exposed to an X-ray film, and then developed; the otherwise invisible probe-marked bands become visible, looking remarkably like a supermarket bar code.

The number of radioactive probes used to bond to the specimen DNA fingerprinting had been used to crack a serious criminal case." Id. See also NOVA: Murder, Rape, And DNA (Nova television broadcast, Mar. 2, 1993).

23. RFLP analysis is probably the most well-known and accepted of the two DNA fingerprinting tests, polymerase chain reaction ("PCR") being the other test. Thompson & Ford, supra note 22, at 48-49. The PCR method is inappropriate for purposes of this proposal. Three major commercial laboratories in the United States currently perform the majority of all forensic DNA typing: Cellmark Diagnostics Corporation, England's first commercial DNA testing laboratory; Lifecodes Corporation in New York; and Forensic Science Associates, using a test developed by Cetus Corporation, in California. Id. In 1991, Roche Molecular Systems purchased the patent for PCR from Cetus for $300 million. ABC News Nightline: Nobel Laureate Biochemist Kary Mullis (ABC television broadcast, Mar. 31, 1994). Cellmark and Lifecodes perform RFLP analysis and Forensic Science Associates performs PCR analysis, sometimes called DNA amplification. Thompson & Ford, supra note 22, at 48-49. See also DiRusso, supra note 14, at 189-91; Moss, supra note 21, at 68-70; Hoefferl, supra note 13, at 471; Jean L. Marx, DNA Fingerprinting Takes The Witness Stand, 240 Sci. 1616, 1616 (1988) [hereinafter Marx Witness]; DNA Fingerprinting And DNA Profiling, Cellmark Diagnostics Marketing Literature (1989). Cellmark is the laboratory responsible for the DNA tests conducted for the O.J. Simpson case. Larry King Live: Evidence In The O.J. Simpson Case (CNN television broadcast, July 26, 1994). The FBI has also established a lab and uses RFLP analysis. Hoefferl, supra note 13, at 472.


25. Franklin-Barbajosa, supra note 22, at 116. The restriction enzymes are proteins that act like molecular scissors to cut the double helix at certain pre-identified points so that many small fragments of double-helix DNA remain. Id.

26. Franklin-Barbajosa, supra note 22, at 117. In order to separate the fragments by length, they are placed on a bed of gel to which an electric current is applied. Id. DNA is negatively charged and moves towards the positive end of the gel. Id. The longer fragments travel more slowly than the smaller fragments, so over several hours, the fragments are arranged by length with the larger fragments nearer their original position in the gel. Id. See also Smith, supra note 21, at 870.

27. Franklin-Barbajosa, supra note 22, at 117. These radioactive probes are single strands of DNA, and they bond with the complementary base pairs of the specimen DNA. Smith, supra note 21, at 871; Hoefferl, supra note 13, at 472.

28. Smith, supra note 21, at 871; Franklin-Barbajosa, supra note 22, at 117. The DNA fingerprint band pattern is "as unique in its way as a normal fingerprint." Kelly et al., supra note 14, at 108.
determines the number of bands on the resulting DNA fingerprint.\textsuperscript{29} When multi-locus probes are used, they produce a band pattern consisting of twenty to thirty bands.\textsuperscript{30} The chance that two unrelated people would have the same band pattern is one in thirty billion.\textsuperscript{31} Some commercial and forensic laboratories currently use computer systems to compare band sizes within band patterns, assisting the examiner in determining matches between specimen DNA profiles.\textsuperscript{32} With minor programming modifications, each individual’s DNA fingerprint could be easily converted to a UPC-type code yielding a unique bar code and a corresponding number sequence.\textsuperscript{33}

C. DNA PROFILING IS ACCEPTED BY THE SCIENTIFIC COMMUNITY

Both the RFLP and polymerase chain reaction (“PCR”) analysis methods for DNA profiling are generally accepted by the scientific com-

\begin{itemize}
  \item PCR analysis is based on gene amplification, and is, therefore, ideal for forensic typing where the amount of DNA may be exceedingly minute or even contaminated. Jean L. Marx, \textit{Multiplying Genes By Leaps And Bounds}, 240 Sci. 1408, 1408 (1988) [hereinafter Marx Multiplying]; Ruth SoRelle, \textit{Anniversary Of A Revolution}, HOUS. CHRON., Sept. 19, 1994, at 6A. The end result of PCR analysis is a single dot when the gene is present in the specimen DNA and no dot if the gene is not present. Kamrin T. MacKnight, \textit{The Polymerase Chain Reaction (PCR): The Second Generation Of DNA Analysis Methods Takes The Stand}, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 287, 307 (1993). A single dot cannot provide the differentiation necessary to the success of this author’s proposal, so further discussion of PCR analysis is beyond the scope of this article. For further information on PCR analysis, see generally MacKnight, \textit{supra}; ABC News Nightline: Nobel Laureate Biochemist Kary Mullis} (ABC television broadcast, Mar. 31, 1994).
  \item Bowne Interview, \textit{supra} note 14.
  \item For an excellent discussion of the differences between and application of single-locus and multi-locus probes, see James H. Bowden, III et al., \textit{A Guide To DNA Fingerprinting—Part 1}, CCN, Feb. 1994, at 3, 3; Sharon Shelton et al., \textit{A Guide To DNA Fingerprinting—Part 2}, CCN, Mar. 1994, at 3, 3.
  \item Cellmark, \textit{supra} note 23, at 4. The Houston Medical Examiner's Laboratory uses eight different probes in forensic DNA typing. Bowne Interview, \textit{supra} note 14. To reach the oft-quoted statistic “one in thirty billion,” Alec Jeffreys and his colleagues made DNA fingerprints of blood taken from twenty unrelated British Caucasians. The twenty DNA fingerprints were laid side-by-side, and the bands were matched by a corresponding band in an adjacent fingerprint. Jeffreys therefore concluded that there is about a twenty-one percent chance that a given band found in a DNA fingerprint will be matched by a band in the fingerprint of an unrelated individual. To calculate the probability that two unrelated individuals will match on all fifteen bands produced by the probe, Jeffreys applied the product rule and concluded that the probability of a coincidental match on fifteen bands was approximately 0.21 or one in thirty billion. Thompson & Ford, \textit{supra} note 22, at 83 (citations omitted).
  \item Bowne Interview, \textit{supra} note 14.
  \item See also Clare M. Tande, \textit{Note, DNA Typing: A New Investigatory Tool}, 1989 DUKE L.J. 474, 481 (1989). Cf. Thompson & Ford, \textit{supra} note 22, at 87 n.188 (stating “DNA print bar-codes are far more blurry and variable than their crisply printed supermarket counterparts”).
\end{itemize}
munity. Commentators admit that both techniques are scientifically acceptable in clinical and diagnostic settings, and the media reports discoveries of new genes virtually every day. Judges, when presented with DNA fingerprint evidence as part of a criminal or paternity case, have found the generation of that evidence generally accepted by the scientific community and, therefore, admissible in accordance with Frye v. United States. Two recent state supreme court decisions exemplify the courts’ acceptance.

In People v. Wesley, the Court of Appeals of New York held that the DNA profile from RFLP analysis is “generally accepted as reliable by the relevant scientific community and was so accepted at the time of the Frye hearing in 1988.”

In State v. Russell, the Supreme Court of Washington-
ton held similarly regarding PCR typing. Since the first use of DNA profiling evidence in Florida in 1988, well over one hundred defendants have been convicted at least partly because of that evidence. Today, most, if not all, paternity contests use DNA profiling to resolve questions of paternity. There may still be some disbelievers in the legal community and in the public at large, but using either DNA analysis process in the medical research laboratory is as familiar to that community as a Bunsen burner.

III. USE OF DNA FINGERPRINTS IN THE HEALTHCARE DELIVERY SYSTEM IS TIMELY

A revolutionary concept is taking root in the healthcare industry—an idea so simple it is taught in kindergarten, a concept so basic that the airline and banking industries would fail without it. The idea is cooperation.

Clinton's healthcare reform plan, although defeated in Congress, did much to foster the healthcare industry's change in attitude from one of competition to one of cooperation. 1994 was a year of double-digit growth to evaluate novel scientific evidence. Id. at 456 (citations omitted). The trial court found that the hearing was necessary. Id.


41. Id. at 765. The defendant was convicted of three counts of murder and challenged "the trial court's conclusion that PCR testing of DNA has gained sufficient scientific acceptance to admit the results of such testing in court." Id. at 755-59. The court found PCR analysis to be in routine use in many settings such as HIV detection and diagnosis, cystic fibrosis and sickle cell anemia detection in neonatal screening, gene replacement therapy, chromosomal abnormalities and mutations detection, and in new fields of molecular anthropology and molecular paleontology. Id. at 765. The court also noted that PCR analysis has been used "to help identify those killed in the Persian Gulf War." Id. See also supra notes 23, 28.

42. Andrews v. Florida, 533 So.2d 841, 850 n.10 (Fla. Dist. Ct. App. 1988) (stating, "[W]hile no appellate court in this country has yet passed on the admissibility of DNA print identification in criminal cases, such evidence has been admitted in civil actions . . . ." (citations omitted)).

43. Lander, supra note 34, at 501. See, e.g., Hopkins v. Indiana, 579 N.E.2d 1297, 1300 (Ind. 1991) (holding that DNA evidence identified defendant as perpetrator and was admissible); Caldwell v. State, 393 S.E.2d 436, 441 (Ga. 1990) (holding DNA identification techniques were "based on sound scientific theory"); State v. Ford, 392 S.E.2d 781, 784 (S.C. 1990) (finding DNA print testing and RFLP analysis to be generally recognized as reliable and generally accepted by the scientific community); Spencer v. Commonwealth, 384 S.E.2d 785, 797 (Va. 1989) (finding DNA testing a reliable scientific technique); People v. Castro, 545 N.Y.S.2d 985, 995 (N.Y. App. Div. 1989) (holding that DNA forensic identification is generally accepted in the scientific community); United States v. Yee, 134 F.R.D. 161, 167 (N.D. Ohio 1991) (holding DNA evidence admissible).

44. Despite extensive research, this author was unable to locate current statistics on the number of paternity cases that depend on DNA profiling.

45. Steven Fox, Legal Issues For Community Health Information Networks, INFOCARE, Sept. 1994, at 38.
in healthcare industry expenditures, the first since the mid-1980s. The new directions of the industry are toward regional healthcare delivery systems with an emphasis on managed care and capitated rates. One healthcare executive claims, "The day of the stand-alone hospital is over." The industry "today is saturated with affiliations, strategic friendships and various other deals where executives of various institutions join to sign on the dotted line." Amidst the backslapping and hype associated with the merger-mania, interaction between and among information systems of new partners is emerging as a compelling and quintessential goal of success in the new industry.

A. SHARING INFORMATION BETWEEN AND AMONG PROVIDERS IS ESSENTIAL

Unlike the "old days," physicians no longer practice medicine in the same town in which they grew up; society has become increasingly mobile. The successful healthcare provider must operate within a different paradigm than its predecessor; the focus has shifted from providing acute, inpatient care at times of crisis to one emphasizing managing health through a combination of preventive and primary care services.

46. Sheldon Dorenfest, 1995 & Beyond: Stepping Around The Pitfalls, HEALTHCARE INFORMATICS, June 1995, at 81. See also John Morrissey, Growth In Information System Expenditures Will Continue, Study Projects, MOD. HEALTHCARE, June 19, 1995, at 74 [hereinafter Morrissey Study] (reporting growth based on annual survey of acute care, nonfederal hospitals). Health care expenditures are predicted to continue to rise to $13 billion by 1997. Dorenfest, supra, at 81. The potential for significant and continuous growth in the industry is important to investment bankers and venture capitalists who regard the industry today as "one of the better investment opportunity areas in the next few years." Id.

47. Dorenfest, supra note 46, at 81. In a study conducted by Sheldon Dorenfest & Associates, almost 70 percent of the 2,900 hospitals housing over 100 beds that were contacted said they had nothing operational on a computerized medical record. Morrissey Study, supra note 46, at 74. Almost one-third of the Chief Executive Officers contacted stated there were no plans at all to implement a computerized medical record system. Id.


50. Morrissey Interface, supra note 49, at 49. No major changes have occurred in most of the currently installed computer systems from those that existed before all the mergers and acquisitions; they date back to an "era in which each department or facility was an island." Id. In the old days, computers were designed to serve the individual unit, not interact with other computer systems in other units. Id.


52. Steven Fox, supra note 45, at 38. "Managing health" should not be confused with "managed care" or "managed competition," terms used to describe the current provider industry. Id. Changes in the provider industry in response to government regulations and
A continuum of seamless, efficient patient care has, or will, replace the fragmented services and use of specialists of yesterday.\textsuperscript{53}

All over the country, healthcare providers are participating in Community Health Information Networks ("CHIN"), becoming part of or forming integrated delivery systems ("IDS") with other providers to provide such care.\textsuperscript{54}

cost containment programs have fostered a radically different approach to healthcare by the patient/consumer—or vice versa. \textit{Id.} One need only open a newspaper or business magazine to read of companies instituting wellness programs, providing incentives to employees to lose weight or stop smoking, or dedicating special facilities for exercise—all in the hopes that the employee with a healthy lifestyle will require less medical care and cost his employer less in healthcare insurance premiums. \textit{See, e.g.,} Dr. Michael E. DeBakey & Dr. William G. Anlyan, \textit{Managed Care Puts Us All At Risk}, \textit{Hous. Chron.}, June 18, 1995, at 1C; Jane Baird, \textit{The Benefits Of Networking}, \textit{Hous. Chron.}, Jan. 22, 1995, at 1E; William H. Cunningham, \textit{Outlook, Managed Care Making Teaching Hospitals Sick}, \textit{Hous. Chron.}, Aug. 17, 1994, at 33A.

\textsuperscript{53} \textit{See Fox, supra} note 45, at 38. The shift in patient focus to managed health results in fewer contacts between the patient and the healthcare industry, as supported by a summary of statistics supporting this contention:

- Patient visits to physicians decreased about 14 percent between 1982 and 1993
- Community hospital occupancy decreased from approximately 75 percent in 1982 to 64 percent in 1993
- HMO enrollee hospital utilization rate was approximately two-thirds of the nation as a whole in 1991
- The number of physician encounters per HMO enrollee was approximately two-thirds that of the nation from 1988 through 1991

\textit{Mara Saltz & Rich Peterson, Bringing Technology Closer To The Patient, Healthcare Informatics, June 1995, at 138.}

\textsuperscript{54} \textit{John Morrissey, Chicago CHIN, Vendors Sign Pact, Mod. Healthcare, June 12, 1995, at 15.} In Chicago, the Metropolitan Chicago Community Health Information Network finalized a contract with its alliance of contractors in June. \textit{Id.} The 500-page contract details expectations regarding security of data, disaster recovery, and response time, but use and payment fees remain undefined. \textit{Id.} Rather than delay the agreement further, the parties decided that trying to establish long-term pricing for something that did not yet exist was impossible. \textit{Id.} The Chicago CHIN expects to have six hospitals on-line and 20 more under contract by the end of the year. \textit{Id.}

In April 1991, the Wisconsin Health Information Network ("WHIN") celebrated its three-year anniversary. \textit{Quietly Marking The Three-Year Milestone, WHIN Management Seeks To Silence Even The Loudest Critics, 1 NO. 2 COMNET's, May/June 1995, at 12.} "WHIN membership now includes more than 1,100 physicians (13% of the state's total), 13 hospitals (9% of the state's total), 50% of the Milwaukee metropolitan-area market, four payor organizations, and numerous other provider groups." \textit{Id.}

Twenty medical offices, 150 physicians, 10 insurance carriers, and numerous laboratories are participating in the Oregon Medical Electronic Network pilot program started this past spring. \textit{OMEN Promises To Connect State, 1 NO. 2 COMNET's, May/June 1995, at 14.}


Sixty percent of the 976 healthcare professionals who took part in the annual HIMSS/Hewlett-Packard Leadership Survey stated that they are now part of a fully-established
Within this changing marketplace, a growing awareness of and emphasis on the need for information sharing has manifested. In order for a CHIN or IDS to operate successfully, it must be able to access the full panoply of records currently scattered throughout its member entities, while using available technology to ensure the security and confidentiality of those records. Since efficient patient care “depends on access to the kinds of data that too often are unavailable,” computer interaction is suddenly Job One. Fortunately, today’s technology is more than capable of handling the challenges created by this need to share information, and the healthcare industry is capitalizing on that capability.

Concurrent with the focus on information-sharing technology is a corresponding emphasis on security of information, and while advances in technology have expanded the dimensions of security, these advances have yet to make a computer completely secure. Comprehensive security delivery system, or are in the process of setting up one. Aldrich & Corley, supra note 10, at 12. No figures on the number of providers participating in CHINs are similarly available, however, activity in this area is high.

According to one legal expert, an IDS is simply one type of CHIN, the other two types being vendor-owned and community coalition. Fox, supra note 45, at 40. The vendor-owned CHIN is usually operated by a vendor for profit, although it may include a joint venture agreement with different providers and payors. Id. Funding for a vendor-owned CHIN is provided by the vendor. Id. A community coalition model is generally operated on a not-for-profit basis by either a coalition or a vendor subcontractor. Id. at 42. Funding is more difficult to obtain and, depending on the members participating in the management decisions, consensus on issues of management and operations may be next to impossible to achieve. Id.

55. See Fox, supra note 45, at 42.
56. INSTITUTE OF MEDICINE, supra note 51, at 32.
57. Morrissey Interface, supra note 49, at 49.
58. Richard S. Dick & William F. Andrew, Point Of Care: An Essential Technology For The CPR, HEALTHCARE INFORMATICS, May 1996, at 64. These authors predict that this year will be the year for computerized patient record systems because of the advance of component technologies essential to their development, “more powerful and affordable hardware, a growing emphasis on mobile, wireless computing, sinking prices for magnetic and optical storage, and advances in user-friendly computer interfaces.” Id. “Technology has been racing to meet healthcare networks at this critical juncture in system development.” Morrissey Interface, supra note 49, at 49 (quoting Andrew Lederer, a senior associate with the Kennedy Group).
59. Morrissey Interface, supra note 49, at 49. Integration challenges facing information executives are somewhat daunting. Id. Many will have to “retrofit their information systems with integration mechanism just to be able to coordinate and share the data within their existing base of computerization.” Id. “Next, they have to round out their roster of information systems to capture and report data that are now committed to ink and paper.” Id. “Finally, the integrated system must be able to accept incremental computer innovation and new network partners, all without upsetting existing operations or squandering previous investment.” Id.
60. Lawrence O. Gostin et al., Privacy And Security Of Health Information In The Emerging Health Care System, 5 HEALTH MATRIX 1, 29 (1995). As technology continues to improve, security of data should correspondingly increase. Id. Nonetheless, comprehen-
A comprehensive security system can significantly degrade system performance and restrict the flow of information in a network environment, which is unacceptable in emergency situations where every second counts. Still, well-established and proven security options are available; these options include password protections at various program and record levels, user identification and authentication capabilities, data encryption, and hardware lock-outs. Ultimate control of information within the shifting marketplace cannot be achieved without first addressing the inherent and unintentional problem; that is, "identification of patients the same way across different information systems."

B. No Standard Identifier Currently Exists

In searching for a uniform patient identifier, the social security number is mentioned frequently as the obvious choice. An identification system based on the social security number would be easy to implement information systems planning will include establishing well-articulated privacy and confidentiality goals to ensure maximum protections. Id.

61. Gostin et al., supra note 60, at 30. Threats to security do not always originate within an organization; protection from unauthorized outside access must also be considered. Id. "Healthcare data is uniquely susceptible to impermissible uses such as creating mailing lists for drug or insurance companies, or permitting financial or employment discrimination." Fox, supra note 45, at 44.


63. See Gostin et al., supra note 60, at 30; Stephanie B. Lichtman, Computers And Privacy Rights: Minimum Standards Needed, 10 NO. 12 COMPUTER L. 26, 27 (1993); Fox, supra note 45, at 44. A software user may have several passwords: one that allows access to the terminal; one that allows access to a particular set of functions in the software; or one that allows access to a particular set of files (such as only those patients on a particular floor or service). Systems may automatically delete passwords on a regular basis. In cases where remote access is necessary, a call-back option provides enhanced security. Passwords are becoming more sophisticated. Voice, retinal scans, fingerprints, and even lip prints are examples of biological passwords used on some computer systems. Rick Tetzeli, Computer Security: New Ways To Keep Hackers Out, FORTUNE, Dec. 16, 1991, at 14.

64. Morrissey Interface, supra note 49, at 54. The current plan to solve the problem of patient identification across systems is to use basic computer-indexing programs currently on the market for now and wait for more high-powered software that is currently under development. Id. Without a resolution to the identification problem, the benefits associated with an integrated healthcare system will remain unrealized. Dorenfest, supra note 46, at 81. The ultimate goal is for the patient to enter a healthcare delivery system at any point and receive "seamless" care across the enterprise. Id. at 81-82.

65. Robert I. Field, Overview: Computerized Medical Records Create New Legal And Business Confidentiality Problems, 11 NO. 8 HEALTHSPAN 3, 6 (1994); Fox, supra note 45, at 44.
Cost-effective and a reliable means of collecting and sharing information. On the other hand, its use is considered dangerous by experts and consumers alike.

In 1936, the government created the nine-digit social security number for the purpose of administering the basic retirement plan for Americans established under the Social Security Act of 1935. Initially, the social security number was intended as "a means to track earnings to determine the amount of Social Security taxes to credit to each worker's account." Over time, however, use of the social security number has become widespread, and the public is becoming increasingly concerned about its potential abuse. In addition to the fact that the social security number is the biggest concern of consumers. Security of personal financial data is the biggest concern of consumers. See Lichtman, supra note 63, at 28. In a recent decision, the Fourth Circuit recognized and supported this concern. Greidinger, 988 F.2d at 1354. In Greidinger, Mr. Greidinger refused to provide his social security number as required by the voter registration laws of the State of Virginia. Id. at 1345. After his application was denied and he was unable to vote in a November general election, Greidinger filed suit to challenge the state's authorization of "the collection and publication of SSN's for voter registration" stating that such provisions unconstitutionally burdened his right to vote and violated the Privacy Act of 1974. Id. at 1345-46. The court recognized "the harm that can be inflicted from
ity number is used in so many places, it is not legally protected, and it is easily linked to unrelated records. The Institute of Medicine of the National Academy of Sciences recommends developing and using a system of unique medical identification numbers “despite the logistical benefits of using an existing identification system.”

The success of any identification number system depends on the uniqueness of the numbers used; a number must be able to “minimize or eliminate the risk of misidentification.” Yet in the healthcare industry, it is also critical that an identifier not unnecessarily impede the prompt

the disclosure of a SSN to an unscrupulous individual [as both] alarming and potentially financially ruinous.” Id. at 1355. The court then listed a few of the uses that an unscrupulous individual could make of another's social security number such as, “obtain[ing] a person's new checks at a new address on that person's checking account, obtain[ing] credit cards, or even obtain[ing] the person's paycheck.” Id. at 1354. A social security number would also “unlock[ ] the door to another's financial records, investment portfolios, school records, financial aid records, and medical records.” Id. Greiding's decision not to provide his social security number was “eminently reasonable” according to the court, which reversed and remanded the case to allow Virginia to cure the constitutionality of its voter registration process. Id. at 1354-55.

For a story that ended in financial disaster for a couple whose credit history was erroneously confused with another individual’s, see Joshua D. Blackman, A Proposal For Federal Legislation Protecting Informational Privacy Across The Private Sector, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 431, 434 (1993).

73. Friedheim, supra note 70, at 843. “[T]he federal government alone maintains more than 856 personal data banks with over four billion computerized records, or about seventeen files for each resident—and it uses the SSN as the identifier to retrieve these records.” Id.

74. Field, supra note 65, at 6. See also Friedheim, supra note 70, at 845 (noting that the social security data system lacks any central control).

75. Field, supra note 65, at 6. See also Minor, supra note 8, at 277-78 (warning of the dangers of “function creep,” which occurs when the social security number, which started off designed for one purpose, adds additional purposes); Friedheim, supra note 70, at 844-45 (explaining the ease of access to data outside one database once it is determined that one key in the database is the social security number).

76. Field, supra note 65, at 6 (citation to Institute of Medicine Report omitted).

77. INSTITUTE OF MEDICINE, supra note 51, at 165. The report states that current software and hardware systems may have to undergo significant modification depending on the format of the unique identifier. Id. The report predicts that extensive reprogramming or forms redesign will be necessary if the unique identifiers have more than 10 digits or characters; the current Medicare identifier is a combination of 10 characters and numbers. Id. Despite these dire warnings, most major hospital information systems currently use code technology in purchasing and inventory modules. Some systems will accommodate bar codes as patient identifiers. In these systems, a bar code is generated for the patient during the admission process and “stored” on the wrist band that the patient wears while in the hospital. When a test or procedure is performed on the patient, the technician will “wand” the bar code associated with the test and then the bar code on the patient's wrist band. The information system then automatically selects the proper patient, test, and associated charge and posts it to the patient's account.
and efficient delivery of healthcare. Further, the identifier must function "anywhere in the country and in any provider's facilities and settings . . . [and] . . . be able to link events that have occurred at multiple providers." Once an individual's DNA fingerprint is reduced to a bar code, the numerical representation of that code easily meets the critical success factors of a unique identification number system. Not only is each individual's DNA unique to him or her, but an individual's DNA is not subject to theft, loss, or fraudulent use by others who might have access to the number. Laboratory specimens are routinely collected from people who receive services within the healthcare delivery system. Even if a person were to "forget" his bar code number, another DNA profile could be generated specifically for that encounter with the healthcare de-

78. INSTITUTE OF MEDICINE, supra note 51, at 167.

79. INSTITUTE OF MEDICINE, supra note 51, at 167. Unlike a card that can be lost, misplaced, or stolen, a person's DNA is always with him. In addition, because each person's DNA is unique and a part of his body, fraudulent use of DNA is virtually impossible. No one can steal another's DNA; if necessary, a DNA test could be a required test for every encounter with the healthcare industry, not just the initial one. Regardless of which facility the person goes to or which provider he sees or how many times he receives medical care, one person's DNA is that person's DNA.

80. See supra notes 28-33 and accompanying text. Bar code technology is more advanced than the simple UPC-code on virtually every grocery item package. Symbol Technologies, has developed a new generation of bar codes "that can accommodate a fingerprint, a photograph, even the Gettysburg Address." Erick Schonfeld, Bar Codes: The Latest Investor Scan, FORTUNE, June 12, 1995, at 141. Traditional bar codes are read horizontally; those developed by Symbol Technologies can be read both horizontally and vertically. Id. For this reason, more than two kilobytes of data can be stored on a single bar code which is "over 100 times that of a traditional code." Id. "The U.S. military is testing the codes on more than one million ID's [which] will contain digitized photos of the holders, along with their blood type, eye color, date of birth, and other personal information that can be read by a scanner." Id. The article reports that several states are starting to use these codes on driver's licenses. Id. Systems designed to convert data to this type of bar code are certainly more advanced than those generating only the horizontal bar code. Using this technology to record a DNA fingerprint will assure a more precise code.

Although DNA is unique from one person to the next, identical twins do share the same DNA. Snyder, supra note 16, at 204; Huber, supra note 15, at 38 n.5; Hoeffel, supra note 13, at 470. When a single fertilized egg splits in two and two human beings result from that process, both will have the same DNA because both actually came from a single fertilized egg. Similarly, identical triplets, quadruplets, quintuplets, sextuplets, and so forth will also have the same DNA. For multiple, identical birth individuals, a prefix or suffix will have to be added to the DNA bar code to be able to distinguish between the medical records. Unfortunately, there is currently no way to "mark" the DNA of one or the other twin so as to distinguish them biologically. With myriad advances in medical science, particularly in the area of gene therapy, however, this might change. See ABC News Nightline: The Scary New World Of Genetic Research (ABC television broadcast, Dec. 16, 1993) (predicting scientists' ability to replace genes sometime within the next decade).

81. See supra text accompanying note 16. To distinguish between the bar code number of identical twins (or in the case of identical multiple births greater than twins), a suffix designating the order of birth will need to be added.
livery system. A subsequent DNA profile would cause little or no inter-
ruption in the individual’s treatment, and could actually yield an 
additional means of identity verification. While costs will be associated 
with establishing a medical identification number system based on the 
DNA profile, the biggest obstacle to adopting such a system is not an 
economic one, but rather overcoming society’s misconceptions and its un-
founded fear of lost individual privacy.

IV. ANALYSIS

A. PERCEIVED CHALLENGES AND OBSTACLES BARRING USE OF THE DNA 
FINGERPRINT AS A UNIQUE PATIENT IDENTIFIER

The public’s first exposure to DNA analysis occurred in 1987 when 
the prosecution in a criminal case presented DNA fingerprinting evi-
dence.82 The defendant was convicted when he offered no rebuttal to 
that evidence.83 Jurors in the case found the DNA test “foolproof,” and 
newspapers likened the DNA fingerprint to a supermarket bar code.84 
Today, despite unquestioned acceptance of the DNA profiling process by 
the scientific community and some courts,85 many legal commentators 
and members of the public at-large remain distrustful of the validity of 
the process or question the resultant statistics that define the odds of a 
match between the suspect’s DNA and the sample DNA.86

B. VALIDITY OF THE DNA FINGERPRINTING PROCESS

The majority of those who criticize the DNA profiling process oppose 
its use in forensics and criminal prosecutions for reasons that are invalid 
in a research or diagnostic environment. Whereas forensic samples from 
which DNA can be extracted are minuscule and usually contaminated, 
research and diagnostic laboratories generally receive more than enough

State’s expert witnesses were skillfully and thoroughly cross-examined, but no expert wit-
ness testified for the defense”).
83. Id.
85. See supra notes 34-44 and accompanying text. Another interesting use of DNA 
testing is about to unfold in Missouri. Two Houston brothers claim kinship with Jesse 
James based on their belief that James was not really shot in Missouri, but lived under an 
alias in Granbury and was buried there in 1951. Allan Turner, DNA May Put Holes In 
Jesse’s Tale, HOUS. CHRON., July 11, 1995, at 1A. Their claim may be settled in the not too 
distant future due to a Missouri judge’s order that a DNA sample be taken from the body of 
the man buried in Missouri and presumed to be Jesse James to prove that the body is 
Jesse’s. Id. If the Missouri body is not James, the Texas brothers will seek a court order 
for exhumation and testing of the Granbury corpse. Id. at 6A.
86. Hoeffel, supra note 13, at 476-94; Hansen, supra note 14, at 229-39; DiRusso, supra 
note 14, at 199-214; Thompson & Ford, supra note 22, at 81-96.
of a specimen extracted under sterile conditions to perform multiple profiles. In addition, research and diagnostic laboratories are required to comply with governmental standards that are inapplicable to their forensic and commercial counterparts.

1. Current Misconceptions About the Process and the Outcomes

Samples used in forensic testing and those used for diagnostic testing are unquestionably different. Besides the obvious difference in volume between forensic and diagnostic specimens, a basic difference in the quality of the samples exists. Forensic samples may be contaminated, degraded, or both; diagnostic samples are rarely contaminated or degraded. The forensic sample may be contaminated by bacteria, plant or animal life, or even human DNA depending on the type of crime. When restriction enzymes are exposed to a contaminated sample, the enzymes might improperly cut the specimen DNA at the wrong location yielding fragments that are not the same length they would be from an uncontaminated specimen of DNA. Similarly, if the specimen DNA is degraded from exposure to the elements or because of time, the fragments may be incomplete, even if the restriction enzymes cut the DNA at the appropriate nucleotide bases, causing erroneous band patterns in the RFLP analysis and, therefore, misleading results. Alternatively, the radioactive DNA probes used during the gel stage of the process may erroneously bind with the bacterial, plant, animal, or human DNA in the contaminated specimen and again create a misleading result. Technicians accustomed to working with the product, however, say there is no such thing as a misleading result; "either the print is correct, or it does not exist."

87. See infra notes 89-92 and accompanying text.
88. See infra notes 100-03 and accompanying text.
89. Hoeffel, supra note 13, at 481-82. In a clinical or diagnostic environment, "the scientist has an unlimited source of DNA and can easily re-perform the test until any possible vagueness is discounted." DiRusso, supra note 14, at 200-01. In addition, rarely is there any contamination in the DNA sample in a clinical or diagnostic environment. Id. at 201.
90. Hoeffel, supra note 13, at 481.
91. Hoeffel, supra note 13, at 482-83.
92. Hoeffel, supra note 13, at 482. PCR analysis is particularly susceptible to this challenge because the bacterial, plant, animal, or human DNA might have contaminated the specimen DNA such that the amplification process produces thousands of copies of the contaminated gene rather than the specimen gene, again leading to erroneous results. Id. Except in cases involving contamination, the age of a sample has no negative effect on its typability. One scientist reports his success in extracting and cloning DNA from Egyptian mummies and mummy fragments over 4,000 years old. Svante Paabo, Molecular Cloning Of Ancient Egyptian Mummy DNA, 314 NATURE 644, 644-45 (1985).
93. Longobardi, supra note 15, at 334-35. At least fifty microlitres of blood (or other bodily fluid) is required to perform an RFLP analysis. Id. at 335 n.82. Where the amount of specimen DNA is inadequate, no results are produced. Id.
A second area of concern expressed by opponents of DNA profiling is the potential bias of the examiner. A computer is used in some laboratories to determine the width of the band patterns on an RFLP analysis, but generally “DNA prints are simply eyeballed to see whether they match.” Opponents of the process believe that if the examiner is not careful, a match may be declared where no match exists. Such a situation occurred in People v. Castro. In Castro, the New York Court of Appeals refused to admit the prosecution’s DNA evidence into evidence because of examiner bias. No other explanation was possible for the examiner’s disregard of bands that were on the DNA profile and creation of bands where there were none.

Whereas forensic DNA samples are manipulated and scrutinized by humans, research and clinical laboratories depend on computers to perform much of the sophisticated and complex laboratory testing and re-
The human error that exists in the forensic laboratory could be virtually eliminated by transferring the process to research and clinical laboratories and using computer systems to read the DNA band patterns and reduce them to a bar code. The need to repeat a DNA profile or determine whether two profiles have matched might never arise in a clinical setting once the initial DNA fingerprint and bar code are established. Only if a patient was unable to communicate, or had no one to speak for or identify him, would the need for subsequent DNA analysis on that patient arise.

The lack of uniform quality control standards, a third area of concern of DNA profiling opponents, is unfounded in the clinical and diagnostic laboratory environment. Clinical and diagnostic laboratories are required to adhere to the strict federal quality control standards of the Clinical Laboratories Improvement Act ("CLIA"). Under CLIA, all laboratory employees must be licensed, a comprehensive set of policies and procedures describing the methodology for every test is required, and detailed quality control programs are made necessary for reagents, instruments, and the laboratory environment. Forensic laboratories, including the three commercial laboratories that perform the majority of DNA testing in the country and the FBI laboratory for DNA profiling, are exempt from CLIA. If the DNA fingerprint is established as the unique patient identifier in the healthcare industry, giving clinical and diagnostic laboratories the responsibility of performing initial DNA analysis and creating DNA fingerprints and the representative bar codes should allay concerns about quality controls and procedures.

The final major area of concern expressed by opponents of forensic DNA profiling is that the statistics used to establish the probability that the defendant was the perpetrator of the crime are invalid. Using a DNA fingerprint as a unique patient identifier will not require any sta-
tistical probability analysis; therefore, further exploration of this area is unnecessary at this time.

2. Costs of Time and Labor Associated with the Process

Today, a complete DNA profile on a forensic sample will take approximately two weeks and cost $300 or more per specimen.\textsuperscript{105} Paternity samples take less time and usually cost half as much.\textsuperscript{106} With a mandatory DNA fingerprint on every person who enters the healthcare delivery system, the initial cost and time involved in taking samples, creating the DNA fingerprint, and reducing that DNA fingerprint to a bar code, would be significant. However, the one-time costs associated with implementing this system must be compared to the potential savings projected to occur over time.

During a routine office visit, a physician will usually order general laboratory tests on a patient, such as a urinalysis and a blood test. If the patient is subsequently referred to a specialist or to a hospital, the same laboratory tests will be duplicated at the new healthcare provider's facility. Part of the reason for duplication is unavailability or inaccessibility of the prior test results to the subsequent provider. If these results were available to the subsequent provider on a healthcare regional information network, such as a CHIN, then repeating tests at the subsequent providers' offices would prove unnecessary. This elimination of duplicative patient tests across healthcare providers in a regional healthcare delivery system would result in immediate, direct, and substantial savings in terms of dollars and time to patients and the healthcare industry.\textsuperscript{107} Additional savings of indirect costs, specifically those associated with duplicate testing and for compiling and transmitting the patient's

\textsuperscript{13}, at 488-92. See also \textsuperscript{105} Lander, supra note 34, at 501-04 (using cases to emphasize problems regarding interpretation of results).

\textsuperscript{105} Bowne Interview, supra note 14. In 1988, Cellmark Corporation charged $285 per sample in criminal cases, requiring two or three samples at a minimum, and $200 per sample in paternity cases, where a minimum of three samples (mother, child, and putative father) are required. \textsuperscript{106} Moss, supra note 21, at 68. In the same year, Lifecodes Corporation charged between $110 and $250 per sample in criminal cases and $110 per sample in paternity cases. \textsuperscript{107} Id. Chemi-luminescence is predicted to replace traditional radiation in creating the final DNA banding pattern, and this technology is faster and less expensive. \textsuperscript{108} Bowne Interview, supra note 14.

\textsuperscript{106} Bowne Interview, supra note 14. Part of the reason for the decreased cost of paternity DNA profiles is that the samples are much larger than their forensic counterparts. \textsuperscript{107} Id. In addition, only one DNA profile per gel is possible with forensic samples whereas multiple profiles can be run on a single gel in paternity cases. \textsuperscript{108} Id.

\textsuperscript{107} See \textsuperscript{109} Gostin et al., supra note 60, at 4. Automation will result in higher quality care, minimize duplicate testing, eliminate paperwork, and foster portability of health coverage. \textsuperscript{108} Id.
medical record to subsequent providers, should also be included considerations of any cost-benefit analysis.

C. OWNERSHIP AND SECURITY OF AN INDIVIDUAL’S DNA FINGERPRINT

If the DNA fingerprint or its bar code equivalent is used as the patient’s unique identifier in the healthcare delivery system, the information would be stored in a database. Obviously, the question of who owns and controls this data becomes paramount. If the federal government owns the process and the data, then some, albeit limited, protection against unauthorized disclosure or access to the information is available. Similarly, if private industry, specifically the healthcare industry, owns the process and the data, then state laws and federal and state regulations provide substantially greater and additional levels of protection against unauthorized disclosure or access. Currently available networking and data base technology provides a third level of protection. Nonetheless, the issues of whether an individual can be forced to submit to DNA testing and, if he can be, whether such submission would infringe on his right to privacy, are questions that must be addressed first. If the answer to either of the above questions is “no,” the issue of ownership and control of a data base is moot.

1. Producing a Specimen for DNA Testing

In 1986, the English police requested, and more than four thousand men in the Narborough area between the ages of thirteen and thirty voluntarily submitted to, blood tests in the hopes of identifying the murderer of two teenage girls.108 One United States reporter attributed the police’s success to the “strong sense of community outrage among close-knit villagers and an effective police public relations campaign [which] effectively overcame apprehensions among some residents that the tests were an invasion of their personal rights.”109 Although such a “genetic sweep” might be acceptable in England, even an overwhelming sense of community outrage might not be sufficient to override an American’s belief in his right to bodily integrity.110

In a criminal trial where admissibility of DNA profiling evidence is at issue, attorneys argue about whether the DNA process was conducted

---

110. Body fluid samples and fingerprints must be given voluntarily in England. De Gorgey, supra note 108, at 386. The only requirement is that the sample be destroyed in the presence of the individual providing it if he is acquitted or not charged. Id. (quoting Peter Thornton of the National Council for Civil Liberties in Britain). “[B]ritish] law [however] says nothing about the information taken from the sample, the data.” Id.
properly or about the validity of population statistics used to evaluate the likelihood of a match between the defendant's DNA and that of the DNA extracted from samples found at or near the crime site. How the defendant was "convinced" to give up his blood, hair, saliva, or skin for DNA analysis receives little or no attention during trial.111 "DNA profiling definitely has potential to violate Fourth Amendment and privacy rights of all individuals"112 in a criminal setting. Yet today, several jurisdictions require convicted sex offenders to give blood and saliva samples for genetic typing as a condition of paroled release.113 Every day, individuals accessing healthcare facilities for treatment, or those seeking employment, "willingly" provide specimens for laboratory testing—specimens that could also be used to create the individual's DNA fingerprint.114

The Fourth Amendment to the United States Constitution guarantees citizens' protection only "against unreasonable searches and seizures."115 In Schmerber v. California,116 the United States Supreme Court held that withdrawing a blood sample for testing blood alcohol levels did constitute a search under the Fourth Amendment.117 Nonetheless, the Court allowed the evidence of Schmerber's intoxication on the basis that the blood test had been performed by a physician and is a

111. Sally E. Renskers, Comment, Trial By Certainty: Implications Of Genetic DNA Fingerprints, 39 EMORY L.J. 309, 323-25 (1990). Identifying a particular individual by his DNA is so exact that when a criminal leaves blood, tissue, or other bodily fluids containing DNA at a crime scene, "it's like leaving your name, address, and social security number at the scene of the crime." Id. at 309 (quoting Michael Baird, citation omitted). DNA has also been successfully extracted from human hair. Russell Higuchi et al., DNA Typing From Single Hairs, 332 NATURE 543, 543 (1988).

112. Smith, supra note 21, at 878.

113. California, Colorado, Virginia, and King County, Washington have passed such laws. See CAL. PENAL CODE § 290.2 (West 1988); COLO. REV. STAT. § 17-2-201 (1988); VA. CODE ANN. § 53.1-23.1 (1989); WASH. REV. CODE § 43.43.754 (1989). In California, the DNA profiles are stored in a computer database. Marcia Barinaga, DNA Fingerprinting Database To Finger Criminals, 331 NATURE 203, 203 (1988).

114. In today's mainstream society, individuals also willingly provide samples of their blood and tissue in order to get hired. See Hoeffel, supra note 13, at 535. Many companies require prospective employees to pass drug screening or AIDS tests prior before they can be hired. Id. at 536.

115. U.S. CONST. amend IV.

116. 384 U.S. 757, 767 (1966). Schmerber appealed his conviction of driving under the influence on several grounds, including his Fourth Amendment right not to be subjected to unreasonable searches and seizures. Id. at 758-59. "He [was] arrested at a hospital while receiving treatment for injuries suffered in an accident involving the automobile that he had apparently been driving." Id. at 758. The police directed a physician to take a sample of Schmerber's blood despite Schmerber's refusal of consent for blood alcohol testing. Id. at 758-59. The test showed Schmerber was intoxicated, and these results were admitted in evidence against him at his trial. Id. at 759.

117. Id. at 766.
procedure that "involves virtually no risk, trauma, or pain." More recently, the Court concluded that collecting and testing a urine sample to determine whether an individual is intoxicated, such testing being performed in compliance with agency regulations, does not violate the Fourth Amendment. Indeed, the Court has never applied the Fourth Amendment prohibition against unreasonable searches and seizures to acts of private individuals. If a patient were to provide blood, tissue, or some other nucleated specimen for specific laboratory tests, and the healthcare facility were to routinely perform a DNA analysis in addition to those tests, the likelihood of the patient's raising a successful Fourth Amendment claim would be doubtful. Whether using a patient's DNA fingerprint is an invasion of his privacy, however, warrants further discussion.

118. Id. at 771. The Court recognized that Schmerber was not "one of the few who on grounds of fear, concern for health, or religious scruple might prefer some other means of testing" so declined to decide whether such grounds, if raised by another, would have to be respected. Id. at 771.

119. Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989). The Federal Railroad Administration's regulations prohibited any employee who was under the influence of, or impaired by, alcohol or a controlled substance from reporting to work. Id. at 608-09. In addition, any employee who was involved in a major train accident or incident was required to undergo blood and urine testing. Id. at 609. In addition, if a supervisor had a "reasonable suspicion" that an employee's acts or omissions contributed to the occurrence or severity of the accident or incident," breath or urine tests or both could be ordered. Id. at 611. Although the Court conceded that collecting and testing urine was an intrusion on an individual's privacy, the Court found the infringement to be insignificant. Id. at 624-25. Further, the Court concluded that even if the infringement had been significant, the individual employee's privacy concerns were outweighed by the compelling governmental interest served by the regulations. Id. at 633. See also Ruth Gavison, Privacy And The Limits Of Law, 89 YALE L.J. 421, 457 (1980) (commenting that an individual's privacy must, at times, give way to "important interests in law enforcement, freedom of expression, research, and verification of data").

120. Wisconsin v. Jenkins, 259 N.W.2d 109, 111 (Wis. 1977). In Jenkins, the defendant was charged with negligent homicide by intoxicated use of a motor vehicle. Id. at 110. At his trial, the State offered results of a blood alcohol test that had been ordered by the treating physician strictly for diagnostic and treatment purposes, but which had not been ordered at the request of police. Id. at 113. Jenkins was unconscious at the time the blood was drawn and did not consent to the procedure. Id. The results of Jenkins' blood test were provided to the police before the complaint against him was issued and prior to his arrest. Id. at 110. Thus, the court found there was no state action in the drawing and testing of the blood such that the exclusionary rule would apply. Id. at 113.

121. The Congressional Office of Technology Assessment confirms that the "seizure[s] of blood, semen, fingerprints, hair, handwriting samples, and other such evidence . . . have been held not to violate the Fourth Amendment or other constitutional prohibitions against forced self-incrimination, if their disclosure is otherwise reasonable." U.S. CONG., OFFICE OF TECH. ASSESSMENT, SCIENCE, TECHNOLOGY AND THE CONSTITUTION 13 (1987).

122. "[A]n invasion of privacy occurs when there is intentional deprivation of the desired privacy to which one is entitled." INSTITUTE OF MEDICINE, supra note 51, at 142-43. Prosser identified four different kinds of privacy invasions: (1) intrusion upon seclusion or
2. The Concept of Informational Privacy

Although everyone generally agrees that a constitutional right of privacy exists, the word "privacy" appears nowhere in the Constitution. Common definitions of privacy include "notions of withdrawal, seclusion, secrecy, or of being kept away from public view." The traditional legal definition of privacy is "the right to be left alone." Countless legal scholars have attempted to further define and refine the definition, and currently, at least three distinct classifications of privacy exist.

The right to "personal autonomy" is the most popular of the three privacy conceptions. This concept includes the right to make decisions about exercising fundamental constitutional rights—a right to control access to oneself. The second most popular concept of privacy is that protection from surveillance or intrusion where an individual has a reasonable expectation of privacy. The third type of privacy, informational privacy, is the individual's interest in controlling personal information about himself or herself so that the information cannot be reached by others. Opponents of DNA profiling warn that it is this solitude; (2) publicity that places an individual in a false light; (3) appropriation of an individual's name or likeness for another's commercial advantage; and (4) public disclosure of private facts. See William A. Parent, Privacy: A Brief Survey Of The Conceptual Landscape, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 21, 24-25 (1995) (referencing William L. Prosser, Privacy, 48 CAL. L. REV. 383, 392-98 (1960)).

123. INSTITUTE OF MEDICINE, supra note 51, at 143. One commentator describes perfect privacy as being "completely inaccessible to others." Gavison, supra note 119, at 428.

124. TOME, supra note 2, at 233. Possibly the oldest definition of privacy was presented by Warren and Brandeis in their article, The Right To Privacy, and by Justice Brandeis in his well-known and often-quoted dissent in Olmstead v. United States. Parent, supra note 122, at 21 n.1-2 (quoting Samuel D. Warren and Louis B. Brandeis, The Right To Privacy, 4 HARV. L. REV. 193, 195, 205 (1890) and Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). See also INSTITUTE OF MEDICINE, supra note 51, at 142-43.

125. INSTITUTE OF MEDICINE, supra note 51, at 143.

126. INSTITUTE OF MEDICINE, supra note 51, at 143. "Autonomy requires the capacity to make an independent moral judgment, the willingness to exercise it, and the courage to act on the results of this exercise even when the judgment is not a popular one." Gavison, supra note 119, at 449.

127. INSTITUTE OF MEDICINE, supra note 51, at 143; Parent, supra note 122, at 22. The fundamental constitutional rights afforded the cloak of privacy include "decisions relating to marriage, procreation, contraception, family relationships, and child-rearing." INSTITUTE OF MEDICINE, supra note 51, at 143. Some use the term "decisional privacy" to describe this right. Id.

128. INSTITUTE OF MEDICINE, supra note 51, at 143. See also supra notes 109-21 and accompanying text.

129. INSTITUTE OF MEDICINE, supra note 51, at 143; Parent, supra note 122, at 22-23. The United States Supreme Court first recognized the value of informational privacy in Whalen v. Roe, 429 U.S. 589, 599-600 (1976).

In Whalen, several physicians and their patients challenged the constitutionality of a New York statute that required physicians to submit the names and addresses of all per-
last type of privacy that is jeopardized. Closer examination of their pro-
fessed concerns, however, reveals only a minimal and non-threatening
loss of individual privacy at best.

The misconceptions about what information a DNA fingerprint con-
tains are the basis for the sometimes hysterical objections to its use as a
uniform identifier. Several commentators warn that an individual's
DNA fingerprint reveals a person's most private information—his or her
genetic make-up—to anyone with access to the fingerprint. With the
warnings come dire predictions of abuse of the information by law en-
forcement officials, insurance companies, employers, schools, adoption

sons who had obtained prescriptions for controlled substances for storage on a centralized
computer file. Id. at 591. The impetus for the legislation was the increasing frequency of
stolen or revised prescriptions which contributed to increased drug abuse. Id. at 592. The
Court recognized that complying with the statute meant that private information would be
disclosed to the state, but held that such disclosure would not "automatically amount to an
impermissible invasion of privacy." Id. at 602. Nonetheless, the Court noted the danger
inherent in requiring such disclosure. Id. at 605.

We are not unaware of the threat to privacy implicit in the accumulation of vast
amounts of personal information in computerized data banks or other massive
government files. The collection of taxes, the distribution of welfare and social
security benefits, the supervision of public health, the direction of our Armed
Forces, and the enforcement of the criminal laws all require the orderly preserva-
tion of great quantities of information, much of which is personal in character and
potentially embarrassing or harmful if disclosed. The right to collect and use such
data for public purposes is typically accompanied by a concomitant statutory or
regulatory duty to avoid unwarranted disclosures.

Id. Because the state had identified, developed, and implemented specific administrative
procedures which evidenced a concern for and protection of individuals' privacy interests,
the Court upheld the statute. Id. at 606.

More recently, a judge in the Supreme Court of Washington identified the four reasons
why informational privacy is so essential to an individual:

First, it preserves the individual's personal autonomy. Second, it facilitates emo-
tional release from the pressures of daily life. Third, it makes possible self-evalua-
tion, including the exercise of conscience. Finally, privacy permits an individual to
engage in limited and protected communication, thus enabling the individual to
share confidences.


130. Burk Testing, supra note 14, at 97. Citizens of this country "already routinely
carry with them a panoply of numerical and photographic identification." Id. Photographs
graphically display an individual's genetic traits, yet virtually no one objects to carrying a
picture identification card, such as a driver's license. Id.

131. See Smith, supra note 21, at 886-87 (predicting creation of new minorities based on
deficiencies in the DNA profile); de Gorgey, supra note 108, at 382-83 (expressing concern
regarding the potential misuse of genetic libraries if they were accessible by employers,
insurance companies, and others); Hoeffel, supra note 13, at 536-38 (predicting that DNA
fingerprinting will threaten an individual's integrity); Renskers, supra note 111, at 346
(recommending that remedies for injuries resulting from release of private information be
tailored to the harm suffered); E. Donald Shapiro & Michelle L. Weinberg, DNA Data
Banking: The Dangerous Erosion Of Privacy, 38 CLEV. SR. L. REV. 455, 469-72 (1990)
(warning that access to a DNA fingerprint will invade an individual's privacy).
agencies, and other organizations, as well as concern that such information will foster a return to the eugenics movement of the 1920's. Such concerns are, for the most part, unfounded. "RFLP patterns actually reveal very little regarding one's genetic make-up." RFLP analysis is directed at the "junk" regions of DNA, which are those regions that "do not appear to contain either coding sequences or genetic control sequences." Further, the bands that appear in an

---

132. Hoeffel, supra note 13, at 533. Being turned down for jobs or insurance, or being denied health insurance or other social services on the basis of the information contained in the DNA profile, are commonly named as the worst of the abuses. Id. See also Burk Testing, supra note 14, at 97; Di Russo, supra note 14, at 217-18; John Shattuck, In The Shadow Of 1994: National Identification Systems, Computer Matching, And Privacy In The United States, 35 HASTINGS L.J. 991, 998-1001 (1984); Jack Kemp & U.S. Sen. Joseph I. Lieberman, National ID Card Would Be A Bureaucratic Nuisance Affecting Everybody, HOUS. CHRON., Aug. 6, 1995, at 5C. Some commentators contend that on-line maintenance and accessibility of DNA profile information will "turn the presumption of innocence into a presumption of guilt." Shattuck, supra, at 1002; de Gorgey, supra note 108, at 397.

133. Hoeffel, supra note 13, at 534. Most Americans ascribe eugenics and compelled sterilization of the socially undesirable or those dependent on the State to the German Nazis. Id. See also Arno G. Motulsky, Societal Problems Of Forensic Use Of DNA Technology, DNA TECH. & FORENSIC SCI. 3, 7 (1989) (this article appeared as part of the proceedings of a conference organized by the Banbury Center of Cold Spring Harbor Laboratory). "[G]eneticists today maintain that political and social use of genetic data in these instances was not based on science but represented pseudoscience of the worst kind." Id.

As recently as 1927, the United States Supreme Court approved sterilization of those considered inferior to the country's enlightened and superior citizens. Buck v. Bell, 274 U.S. 200, 207 (1927). Justice Oliver Wendell Holmes, writing for the majority, stated, We have seen more than once that the public welfare may call upon the best citizens for their lives. It would be strange if it could not call upon those who already sap the strength of the State for these lesser sacrifices . . . in order to prevent our being swamped with incompetence . . . . The principle that sustains compulsory vaccination is broad enough to cover cutting the Fallopian tubes. [citations omitted] Three generations of imbeciles is enough.

Id. By 1956, more than 58,000 citizens had been sterilized under the Model Eugenics Act. Hoeffel, supra note 13, at 534. "In 1966, at least twenty-three states still had not repealed their sterilization laws and at least ten states still provided for sterilization of epileptics and criminals." Id. (citation omitted). State laws that mandated testing for sickle-cell anemia were actually a form of negative eugenics, designed to discourage marriage to carriers of the disease. Id. See also Smith, supra note 21, at 885-86 (using mandatory sickle-cell testing as a tool to discriminate on the basis of ethnicity). These laws fostered racial discrimination of African-Americans, the primary carriers of the gene, who were denied employment opportunities and charged higher insurance premiums. Id. at 534-35.


135. Burk Testing, supra note 14, at 94. Dr. Sydney Brenner, Director, MRC Molecular Genetics Institute states, "The difference between junk and garbage is exactly the same as the difference you make—namely, that garbage you throw away and junk you keep because you think you might want to do something useful with it, and of course, you never do." NOVA: Decoding The Book Of Life (NOVA television broadcast, Oct. 31, 1989). RFLP analysis is directed at those polymorphic areas of DNA that currently have no known function, yet it may only be a matter of time before the functionality of the regions is determined. Burk Testing, supra note 14, at 94.
RFLP banding pattern are a direct result of which DNA probe is used.\textsuperscript{136} In order to use the banding pattern for additional sensitive genetic information, scientists must first develop DNA probes for those specific genetic traits.\textsuperscript{137} Obviously, the most sensitive genetic characteristics are those relating to personality disorders, psychopathy, and criminality.\textsuperscript{138} Knowing whether an individual possesses one or more of these particular characteristics would, indeed, be invaluable information for an employer, an insurance company, or law enforcement. Clearly, the owner of such

\textsuperscript{136} Bowne Interview, supra note 14. See also Motulsky, supra note 133, at 5 (extracting information from DNA profile requires using specific DNA probes).

\textsuperscript{137} Motulsky, supra note 133, at 5. Only 3 percent of all DNA is actually genes. Carey et al., supra note 13, at 74. Stated differently, scientists have not identified 97 percent of the genetic material that makes a human being what he or she is. Even when all of the genetic material is identified and scientists have constructed a map of the human genome, the interactions between the genes will still be unknown.

In 1990, the Human Genome Project ("HGP") was formally launched. Cassel & Levinson, supra note 15, at 11. Its objective: "the mapping and sequencing of the human genome." James D. Watson, The Human Genome Project: Past, Present, And Future, 248 Sci. 44, 44 (1990). Given their success in determining complete DNA sequences in small DNA viruses and in a large number of individual genes, scientists believed that determining the make-up of the human genome was not only possible, but would help them understand the functioning of a healthy human being and explain the role of genetic factors in critical diseases such as cancer, Alzheimer's disease, and schizophrenia. \textit{Id.} At its inception, the HGP was projected to take at least 15 years to complete and cost $3 billion. Carey, supra note 13, at 75; Burk Testing, supra note 14, at 93; Watson, supra, at 44. Early in the Project's existence, "J. Craig Venter, an obscure National Institutes of Health scientist, perfected a method to rapidly find and sequence genes." Carey, supra note 13, at 73. Rather than attempt to sequence the entire 3 billion individual molecules of DNA, Venter's approach was to ignore the junk DNA and copy only the DNA of important genes. \textit{Id.} at 75. His approach "cut the cost of sequencing an unknown gene from an estimated $50,000 using older methods to roughly $20." \textit{Id.}

As of 1995, 85 to 90 percent of all human genes have been sequenced. \textit{Id.} at 77. By 2002, three years prior to its original projected completion date, scientists predict to complete the sequencing of the human genome. \textit{Id.} However, whether scientists could take the next step—genetically engineer a human—is doubtful. \textit{ABC News Nightline: Could We And Should We Recreate The Dinosaur?} (ABC broadcast, June 10, 1993). Ward Wheeler, molecularbiologist, explains,

\begin{quote}
We have to start with naked DNA and assemble it in the right way, coil it up in the chromosomes, and then turn these chromosomes and genes on in exactly the right order and the right sequence, and then let this follow all the way through development. The problem is that we'd have to control all these processes, that we have a dim glimmer of how they actually operate right now. . . . [E]ven this is really beyond our grasp.
\end{quote}

\textit{Id.}

\textsuperscript{138} Motulsky, supra note 133, at 5. More and more DNA probes are becoming available, but these newer probes define "marker genes"—genes that are linked to some gene of interest. \textit{Id.} "The detection of . . . a main gene via its linked marker usually requires investigation of several family members." \textit{Id.} Families with manic depressive and schizophrenic disorders and Alzheimer's disease are examples of traits that may be evidenced by linked marker genes. \textit{Id.} (citations omitted).
discreet information would possess greater power over the individual than someone without the information. However, whether these traits are determined by one gene, a combination of genes, or some interaction between genes and the individual's environment is not known at this time. Since so little is known about such sensitive genetic characteristics, "no probes for such traits exist." Without a "specific" probe, no specific information is provided to the observer of a DNA profile. Thus, in reality, a banding pattern provides no "secret" information so is, at most, useful only for identification purposes.

3. Ownership and Control of DNA Fingerprint Databases

Proliferation of data bases is a fact of life in today's technology-driven world. As technological advances and improvements continue to occur, "the opportunity will grow for DNA fingerprints to operate as passwords or identifying numbers, in national information data banks." Without a doubt, use of the DNA fingerprint as the unique patient identifier will facilitate accessibility, integration, verification, and transmission of electronically stored and maintained patient records, so the importance of individual privacy and security of these records cannot be ignored. Whether ownership and control of the data base containing DNA fingerprints should vest in the federal or state government, or in private industry, must be decided by which option provides the best protection against wrongful disclosure of the information.

Without a doubt, Congress recognizes the individual's right to informational privacy. In the past thirty years, Congress has enacted at least ten privacy laws, including the landmark Privacy Act of 1974. Six years prior to its enactment, Congress passed the Freedom of Infor-

---

139. Motulsky, supra note 133, at 5. "[M]any of the genome project's staunchest advocates are skeptical that we will ever understand complex traits like intelligence through deciphering the book of life [DNA], since they depend inextricably on both nature and nurture." NOVA: Decoding The Book Of Life (NOVA broadcast, Oct. 31, 1989).
140. Motulsky, supra note 133, at 5.
141. Burk Testing, supra note 14, at 94.
142. Lichtman, supra note 63, at 28.
143. Renskers, supra note 111, at 345. Ms. Renskers raises the dangers associated with using any unique identifier in a nationally accessible data base, including unauthorized entry, access, or storage of information. Id. Potential hardware or software failures must also be considered since these could significantly and negatively impact the use and validity of the medical records themselves.
144. Gostin et al., supra note 60, at 5.
145. Blackman, supra note 72, at 445.
146. Lichtman, supra note 63, at 27. See also Blackman, supra note 72, at 445 (reviewing federal laws that protect informational privacy); Arnold, supra note 2, at 475-76 (presenting foundations of privacy in the medical record found in federal and state laws).
DNA AS A UNIQUE PATIENT IDENTIFIER

Information Act ("FOIA"). Disclosure of such records is mandatory, unless the requested material falls under one of nine exemptions: "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" is one of the exemptions. While the FOIA allows any individual access to virtually any record, the Privacy Act of 1974 restricts disclosure of records to any person or entity without the express knowledge and consent of the person who is the subject matter of the inquiry. Agencies that gather data must notify individuals that the data is being collected, explain why it is being collected, and inform them as to whether disclosure is mandatory or voluntary. In addition, each individual has the right to access and correct his records and the right to administrative review if the agency refuses to amend them. Nevertheless, the Privacy Act of 1974 does not prohibit disclosing an individual's record without his consent if the disclosure is made: to agency employees maintaining the rec-

150. 5 U.S.C. § 552(a) (1995). Congressional findings regarding existing statutory regulations stated:

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal Agencies;
(2) the increasing use of computers and sophisticated information technology while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;
(3) the opportunities for an individual to secure employment, insurance and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
(5) in order to protect the privacy of individuals identified in information systems maintained by Federal Agencies it is necessary and proper for Congress to regulate the collection, use, and dissemination of information by such agencies.

Grossman, supra note 8, at 1023.
151. The Privacy Act of 1974 “prevents a federal agency’s disclosure of information pertaining to an individual unless the individual has made a request or has given consent to disclosure in writing, or unless disclosure is provided for under the exceptions to the Privacy Act.” St. Michael’s Convalescent Hosp., 643 F.2d at 1372. See also Arnold, supra note 2, at 475-76 (recognizing release of confidential information is subject to a balancing test between individual’s privacy rights and the public’s right to information).
153. 5 U.S.C. § 552a(b) and (d) (1995).
ord; to individuals with advance written assurance that the record will be used in statistical research; to U.S. agencies charged with enforcing civil or criminal law; or, to persons who demonstrate compelling circumstances affecting the health or safety of another.  

The safeguards provided under the FOIA and the Privacy Act of 1974 are significant. However, by themselves, these safeguards would not offer sufficient protection against wrongful disclosure of an individual's medical record if such disclosure is made by a healthcare provider or healthcare entity. First, both the FOIA and the Privacy Act of 1974 apply only to "agencies" as defined under 5 U.S.C. § 551(1). Second, there is no private right of action to enjoin agency disclosures of information under either Act. Finally, even though virtually every healthcare facility receives some federal funding, the courts refuse to make acts of federally funded healthcare facilities acts of the federal government.  

Many of the inherent flaws in the FOIA and the Privacy Act are addressed in the Fair Health Information Practices Act ("FHIPA") of 1994, but FHIPA has not yet been enacted. Whether FHIPA will be passed in the near future is questionable. FHIPA was created to complement and support national healthcare reform; its provisions protect individual privacy and ensure information confidentiality.  

A necessary component
of healthcare reform would have been some sort of national identification card.\textsuperscript{159} Since the defeat of Clinton's Health Security Act,\textsuperscript{160} the perceived need for FHIPA has correspondingly diminished—unfortunately for the private individual and the evolving healthcare networks.

State governments are in no better position to take responsibility for maintaining a secure and confidential medical records database.\textsuperscript{161} "[N]o two states have adopted the same standards of confidentiality or the same procedural safeguards."\textsuperscript{162} What constitutes confidential information varies from state to state; only thirty-one of the fifty states specifically protect medical records.\textsuperscript{163} The existing inconsistency between the countability to those who use and disclose data. \textit{Id.} Patients would be informed of "the intended uses of their medical information, [given] the opportunity to inspect, copy and correct their records, . . . disclosure [of the records would be limited to the minimum necessary to accomplish an intended purpose, and . . . strong security measures restricting access [would be required of holders of records]." Field, \textit{supra} note 65, at 6.

159. FHIPA, introduced by Representative Gary Condit, envisioned the creation and use of health information trustees who, in order to fulfill their fiduciary duty to the patient, would adopt “fair information practices throughout a modern healthcare system.” Gostin et al., \textit{supra} note 60, at 12. These practices “would establish a system of unique individual identifiers for participants in health plans.” Field, \textit{supra} note 65, at 5. More importantly, however, linking health care information with other information would be strictly prohibited in order to foster information confidentiality. \textit{Id.}


161. State laws can be relatively specific and strict in protecting confidentiality of a medical record. \textit{See infra} notes 162-64 and accompanying text. However, state laws protect the flow of medical information within a state, and “medical information is rarely restricted to the state in which it is generated.” Gostin et al., \textit{supra} note 60, at 16. Medical consultations, research collaborations, and federal governmental regulations require a free flow of medical information outside the state. \textit{Id.} In addition, the physical location of health information is no longer a relevant consideration for development of privacy policies. Databases containing huge quantities of health information provide the potential for immediate access by a variety of eligible users in remote locations. Thus, state laws that attempt to regulate information physically contained in a particular state are anachronistic vestiges of a pre-electronic era.

\textit{Id.}


163. Goldstein, \textit{supra} note 162, at Appendix III. The states that define and afford specific protection to the medical record include Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Idaho, Illinois, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Washington, West Virginia, and Wyoming. \textit{Id.} Mr. Goldstein classifies the aforementioned states as
states makes access to a particular piece of information easy for one who wants it—he need only find a state that “either does not consider the record confidential, or that makes little effort to stop disclosure of confidential data” and access the record from that state.\textsuperscript{164} Since information, once disclosed, can be transmitted faster and to more places than the releasing entity can determine and subsequently correct, injunctions and administrative remedies, if available, are usually too late to afford the injured party any remedy.\textsuperscript{165}

4. Maintaining DNA Information in the Healthcare Industry

In contrast to the aforementioned problems with federal or state government ownership and control of DNA fingerprints, the healthcare industry is ideally suited to be the creator, owner, and manager of a database containing DNA fingerprints.\textsuperscript{166} In order to use the DNA fingerprint as the patient’s unique identifier on his or her medical record,\textsuperscript{167} a specimen from which the patient’s DNA can be extracted must first be submitted to the laboratory performing the DNA analysis. The appropriate specimen can be collected from each patient for DNA profil-

---

\textsuperscript{164} Goldstein, supra note 162, at 1205.

\textsuperscript{165} Goldstein, supra note 162, at 1205.

\textsuperscript{166} Since each patient's DNA profile would be the identifier for his or her medical record, no specific DNA fingerprint database is necessary; the healthcare entity's existing clinical databases will be modified to change the current medical record number to that of the DNA bar code or, in some instances, augmented to include the DNA bar code where access to the patient's record is by some code other than the medical record.

\textsuperscript{167} “The main purpose of the medical record is to accurately and adequately document a patient’s life and health history, including past and present illness(es) and treatment(s), with emphasis on the events affecting the patient during the current episode of care.” Edna K. Huffman, Health Information Management 30 (Jennifer Cofer, ed., 10th ed. 1994). A patient’s medical record “may be written, typed, or computer generated.” Roach et al., supra note 2, at 1. Using a computerized medical record system will enhance its completeness and accuracy and provide immediate and simultaneous availability to authorized personnel. \textit{Id.}
The resulting DNA fingerprint will then be converted to its bar code representation. Next, this bar code will be further reduced to a series of numbers that represent banding patterns of the DNA profile. Since the bar code will actually be a numerical representation of a laboratory value, using the value is an express disclosure of personal information. Some individuals may consider disclosure of the value, even if made only to members of the healthcare providers who are authorized to receive the information, to be a loss of their informational privacy. A court, however, would likely find such a loss to be minimal and insignificant.

The numerical representation of the bar code would serve as each patient's unique medical record number, remaining constant throughout the individual's life. The medical record, now identified by an identifier unique to an individual patient, would reside on the appropriate CHIN database, subject to transfer to alternate CHIN's upon request or when the individual relocated. The inherent protections afforded medical...
records in the healthcare industry, the industry's current traditions, and existing state and federal statutes and regulations would automatically attach to the DNA bar code, satisfying the patient's expectations of confidentiality in both his code and medical record information. Further, since the DNA bar code would only be used for medical records purposes, attempts to access non-medical personal information using only the DNA bar code would be difficult, if not impossible.

In order to create a DNA fingerprint, a laboratory must perform DNA analysis on an appropriate specimen collected for that purpose. Most hospitals and large physician group practices or clinics submit all, or the majority, of their patient laboratory tests to their on-site clinical laboratory. As mentioned previously, when the DNA analysis procedure is attacked in court, the challenge is at least partially based on questions of a laboratory's improper or inadequate standards, procedures, or quality control or on the technician's inability to adequately perform the process. Under CLIA of 1967, every clinical laboratory is required to be certified by the Secretary of the Department of Health and

blocks On The Information Superhighway, 41 Fed. B. News & J. 495 (1994). The National Research Council recognizes that “digital communications can be easily intercepted and manipulated by people, groups, or national governments intent on committing fraud, espionage, or malicious acts.” Id. at 495-96. As Americans have become increasingly dependent on computers, the vulnerability of these systems has become increasingly apparent. Id. at 496.

[Computers] control power, delivery, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Id. Mr. Banisar proposes a return to “a modern version of the 4,000-year-old technique of cryptography—the scrambling of information into an unreadable language that only the intended recipient can understand” as a means of ensuring “that individuals’ privacy is protected, companies’ trade secrets are secured, and financial fraud is prevented.” Id. His article also thoroughly explores the history and current status of federal legislation regarding computer information security.

173. Many healthcare facilities send patient specimens to reference (outside) laboratories if the test that was ordered is not routine, an abnormal result is anticipated, or an epidemiological risk associated with not alerting proper health authorities exists.

174. See supra notes 87-103 and accompanying text. For an in-depth review of the standards, requirements, and guidelines that a clinical laboratory must follow in order to become certified or renew its certification, see generally MORAN & CROLLA, supra note 102. Drs. Moran and Crolla offer a step-by-step approach to participating in and successfully completing laboratory inspection. Id. A sample of their recommendations include the following:

(1) Implement an on-going Quality Assurance (QA) program which will begin with the physician ordering the test and continue through the collection, handling, and analysis of the sample and through reporting the results to the ordering physician.

(2) Develop measurement systems to monitor quality control and proficiency testing.
Human Services. Standards defined in CLIA govern the number, types, and methodologies of laboratory examinations and other procedures performed, as well as laboratory personnel qualifications. If clinical laboratories are responsible for conducting the DNA analysis on every patient, CLIA provisions will eliminate virtually all of the complaints about the profiling process itself; quality controls and standards for DNA profiling will exist, and technicians will have to maintain a certain level of competency. Most importantly, the strong confidentiality obligations of the healthcare industry to patient medical records will inure to the individual's informational privacy interest in his DNA fingerprint, however minimal the interest.

(3) Establish criteria that define when specimens submitted for testing are unacceptable
(4) Monitor and challenge inconsistent results
(5) Establish policies to ensure employee competency and then evaluate employee performance in a timely fashion
(6) Establish procedures to assure accurate reporting, transmittal, storage, and data retrieval and to investigate complaints from customers
(7) Establish and follow regular preventative maintenance schedules for laboratory equipment

Id.

175. Under the Clinical Laboratory Improvement Act ("CLIA") of 1967, a "laboratory" or a "clinical laboratory" is defined as a facility for the biological, microbiological, serological, chemical, immuno-hematological, hematological, biophysical, cytological, pathological, or other examination of materials derived from the human body for the purpose of providing information for the diagnosis, prevention, or treatment of any disease or impairment of, or the assessment of the health of, human beings.


176. Clinical laboratories may be issued or renew a certificate upon filing an application that describes the characteristics of the laboratory examinations and other procedures in the laboratory including:

(i) the number and types of laboratory examinations and other procedures performed,
(ii) the methodologies for laboratory examinations and other procedures employed, and
(iii) the qualifications (educational background, training, and experience) of the personnel directing and supervising the laboratory and performing the laboratory examinations and other procedures.


177. If a laboratory does not comply with the requirements of CLIA, the Secretary may impose intermediate sanctions, examples of which include money penalties, costs for on-site monitoring, directing the plans for correction, or a combination of all of the above. 42 U.S.C. § 263a(h) (1988 & Supp. 1994). More serious violations might result in suspension, revocation, limitation of the certificate, or an injunction, if continuation of the laboratory's activities posed a significant hazard to public health and safety. 42 U.S.C. § 263a(i) and (j) (1988 & Supp. 1994).

5. Protections Against Unauthorized Disclosure of Sensitive Medical Data Exist

The patient believes that his medical record and its contents are confidential; someone has a duty either not to disclose information from the medical record or to prevent unauthorized access to that information by others. This perception is due partially to the public's understanding (or misunderstanding) of professional promises of confidentiality and partially to interpretations of state and federal laws and regulations.

The patient who discloses private and personal information to a healthcare professional assumes that the healthcare professional will not disclose the information to anyone else without the patient's consent. Adopted in the fourth century B.C., the Hippocratic Oath forms the basis for this assumption:

Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things as to be as sacred secrets.

This assumption is further supported by the knowledge of the physician-patient privilege, legally protected in more than forty states, but

179. See INSTITUTE OF MEDICINE, supra note 51, at 145. “Confidentiality is the underpinning of the legal aspects of medical records.” HUFFMAN, supra note 167, at 576. Defined more simply, “confidentiality means keeping a secret.” Id. at 577. However, absolute medical confidentiality does not exist, but ethically, if not legally, unauthorized disclosure or use of the medical record is strictly prohibited. Id. See also Hague v. Williams, 181 A.2d 345, 349 (N.J. 1962) (holding that a patient's right against the physician for disclosure of personal information is a limited right that is balanced against the interests of society in the information).

180. Gostin et al., supra note 60, at 15-16.

181. Oath of Hippocrates, 4th century B.C. The Hippocratic Oath justifies confidentiality on the grounds of respect for privacy. INSTITUTE OF MEDICINE, supra note 51, at 148. At least one court acknowledged the promise of discretion in the Hippocratic Oath as an express warranty of silence. Hammonds v. Aetna Casualty & Sur. Co., 243 F.Supp. 793, 801 (D.N.D. Ohio 1965). Violations of that warranty are no different than violations of obligations under a contract. Id. The district court stated, “Nothing material is more important or more intimate to man than the health of his mind and body.” Id.

“...if information concerning a patient’s mind and body [is] viewed as [an] extension [ ] of the patient, then the concept of autonomy requires that the patient be able to control disclosure and use of that information.” Id. Justice Cardozo articulated this concept of patient autonomy in 1914 when he wrote, “Every human being of adult years and a sound mind has a right to determine what shall be done with his own body.” Schloendorff v. Soc'y of New York Hosp., 105 N.E. 92, 129 (N.Y. 1914).

182. Despite its recognition, not all information provided by the patient is subject to the duty; only that relating to the “patient's health status or other highly sensitive or personal matters that the patient would not have disclosed if the patient had not sought medical treatment would qualify as confidential.” Gostin et al., supra note 60, at 20. Nonetheless, information disclosed to a physician is treated as presumptively confidential. Id. The American Medical Association's Principles of Medical Ethics provides,
still the subject of much litigation. In perhaps the first case to test the boundaries of the privilege, the Supreme Court of Nebraska held that a physician who disclosed that his patient had syphilis was privileged to “make so much of a disclosure to such persons as is necessary to prevent the spread of the disease.” Although recognizing the highly confidential nature of the physician-patient relationship, the court determined that no betrayal of patient confidentiality occurred since the patient knew or should have known when he received treatment that his highly contagious disease might be disclosed.

A physician may not reveal the confidences entrusted to him in the course of medical attendance, or the deficiencies he may observe in the character of patients unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or the community.


183. Hiller, supra note 148, at 470. The physician-patient privilege did not exist at common law. R.K. v. Ramirez, 887 S.W.2d 836, 839 (Tex. 1994). Further, the privilege is a legal concept that only protects the professional from “having to testify in court about medical treatment and the content of all communications related thereto without the consent of the patient.” Hiller, supra note 148, at 470. See, e.g., R.K., 887 S.W.2d at 839-40 (finding a physician’s alleged malpractice insufficient to warrant release of the physician’s mental health treatment information to the plaintiffs); Ex parte Abell, 613 S.W.2d 255, 263-63 (Tex. 1981) (holding the physician-patient privilege protects the patient against an invasion of privacy); Falcon v. Alaska Pub. Offices Comm'n, 570 P.2d 469, 478 (Alaska 1977) (extending the confidentiality of the physician-patient relationship to areas outside medical advice or professional judgment); Horne v. Patton, 287 So.2d 824, 831 (Ala. 1973) (finding the physician-patient relationship to be an implied contract); Rudnick v. Superior Court, 523 P.2d 643, 649-50 (Cal. 1974) (authorizing third parties to whom a physician discloses confidential information on behalf of the patient to hold and assert the privilege); Scheffey v. Chambers, 790 S.W.2d 879, 881 (Tex. Ct. App.—Houston [14th Dist.] 1990) (distinguishing between offensive and defensive use of physician-patient privilege).

When physician-patient communications threaten the health or safety of third parties, the interests of those third parties outweighs the privacy interests of the patient, and communications may then be disclosed. See Simonsen v. Swenson, 177 N.W. 831, 832 ( Neb. 1920). See also Humphers v. First Interstate Bank of Oregon, 696 P.2d 527, 535 (Or. 1984).

184. Simonsen, 177 N.W. at 832. The plaintiff was working out of a small Nebraska town and went with three other men to “a small hotel operated by a Mrs. Bristol.” Id. at 831. While staying at the hotel, he developed sores, which prompted him to seek medical treatment from the practicing physician in the town. Id. The physician stated that he believed that the plaintiff had syphilis, but a Wassermann test was necessary for positive diagnosis. Id. He also told the plaintiff that, because of the contagious nature of the disease, it would be best for him to leave the hotel. Id. When the plaintiff refused to leave, the physician advised Mrs. Bristol of the need for extreme care in dealing with the plaintiff and his belongings. Id. “Mrs. Bristol, acting upon this warning, placed all of plaintiff’s belongings in the hallway, and fumigated his room.” Id. The plaintiff had no choice but to leave and, upon leaving the town, consulted another physician and was given a Wassermann test which proved to be negative. Id.

185. Id. at 832. The court also found the physician to have acted in good faith and without malice. Id. But see Humphers, 696 P.2d at 536 (holding a physician’s release of medical record information to an individual is a breach of confidentiality and invasion of the patient’s privacy). In 1959, an unmarried woman gave birth to a girl who she immedi-
Once the patient provides confidential information to a healthcare professional and that information is transcribed into the patient's medical record, the record holder's privilege to disclose the information becomes a question of weighing the individual's privacy rights against the interests of the third party seeking the information. In the landmark case of [citation], the court found that "the physician's duty to keep medical and related information about a patient in confidence [to be] beyond question." In [citation], the court said there is "no privilege to disregard the professional duty imposed by the Oregon statute solely in order to satisfy the curiosity of the person who was given up for adoption." In [citation], the court stated:

186. See Arnold, supra note 2, at 480-81. "For example, society's interest in controlling the spread of AIDS and developing more efficacious treatment may outweigh an individual's interest in preventing the disclosure that she has the disease." Id. at 480. Cf. Rasmussen v. South Florida Blood Serv., Inc., 500 So.2d 544, 537-38 (Fla. 1978) (denying discovery of names and addresses of blood donors whose blood might have been the source of AIDS contracted during a blood transfusion).

When the patient puts his medical condition at issue, his medical records may no longer be protected. See Fiore v. Lynch, 637 A.2d 1052, 1055 (R.I. 1994). Nevertheless, portions of medical records not relevant to the patient's physical, emotional, or mental condition may not be disclosed. Groves v. Gabriel, 874 S.W.2d 660, 661-62 (Tex. 1994). Likewise, parents who apply for life insurance on their baby cannot protest when the physician conveys relevant medical information that might impact their application to the insurance company writing the policy. Hague v. Williams, 181 A.2d 345, 346-48 (N.J. 1962). However, if a patient authorizes the release of her own psychiatric medical records for litigation purposes, the court usually orders the hospital to provide them. Cynthia B. v New Rochelle Hosp. Med. Ctr., 458 N.E.2d 363, 369 (N.Y. 1983). In Cynthia B., however, the New York Court of Appeals did recognize the possible danger of "self-fulfilling diagnoses" and cautioned against automatic disclosure of a patient's psychiatric records solely upon the patient's waiver. Id. at 367-68. However, when the medical records of a non-party patient are requested so a party patient can determine from those records the movements of the treating physician, the court must assert the privilege against disclosure on behalf of the non-party patient and examine the records to determine whether such disclosure can be made without infringing on the non-party patient's privacy rights. Tucson Med. Ctr., Inc. v. Rowles, 520 P.2d 518, 523-24 (Ariz. Ct. App. 1974).

Names and addresses of disabled officers obtained from their medical records are considered public information under the FOIA. See Disabled Officer's Ass'n v. Rumsfeld, 428 F.Supp. 454, 459 (D.D.C. 1977). The Internal Revenue Service is able to reach not only names and addresses, but dates of treatment and methods of payments for patients of a physician under investigation by the IRS. See Barrett v. Quipu Invs., N.V., 738 S.W.2d 16, 18 (Tex. Ct. App.—Houston [1st Dist.] 1987). In an insurance fraud investigation conducted by Pennsylvania Blue Shield and Medicare, disclosure of entire medical records of patients of the physician who was the subject of the investigation were ordered, although the court sealed the records to maintain the patients' confidentiality. In re Search Warrant (Sealed), 810 F.2d 67, 69 (3d Cir. 1987). Similarly, when medical records information was crucial to an investigation of licensed physicians for medical misconduct, the court ordered
case, United States v. Westinghouse Electric Corporation, the Fourth Circuit established a seven-prong test to determine when "intrusion into an individual's privacy is justified" and, thus, medical records information can be disclosed. Given the potential health and safety risks in


On the other hand, an insurance company's "Authorization to Release Information" does not allow the release of medical information to others. Alpha Life Ins. Co. v. Gayle, 796 S.W.2d 834, 836 (Tex. Ct. App.—Houston [14th Dist.] 1990). In an interesting opinion, the Supreme Court of Minnesota held that a hospital's patient information operator's statement to a caller that a particular patient had been discharged after giving birth was not a breach of patient confidentiality. Koudsi v. Hennepin County Med. Ctr., 317 N.W.2d 705, 705 (Minn. 1982). In Koudsi, a mother, pregnant by a man other than her husband, decided to keep her pregnancy confidential and give her baby up for adoption because she was attempting to reconcile with her husband. Id. at 706. When she entered the hospital, only her sister and the adoption society were aware she was pregnant. Id. After her baby was born, the mother specifically notified the floor nurse that "she wanted her presence in the hospital kept confidential." Id. The mother further communicated her wish for confidentiality to the head nurse and even requested that the baby be moved to the back of the nursery so that the card on the bassinet that identified the baby as hers would be less visible. Id. After the mother was discharged, a different sister called the hospital to inquire about the mother's status having been told that the mother had gone to the hospital for stomach tests. Id. In response to the sister's inquiry, the operator told her that the mother had been discharged "but that the baby had 'stayed behind.'" Id.

One court recently concluded that the "need for confidentiality does not necessarily mean that a statute requiring disclosure [of medical information] would violate the federal constitution." Peninsula Counseling Ctr. v. Rahm, 719 P.2d 926, 928 (Wash. 1986). In Peninsula Counseling, the Supreme Court of Washington refused to enjoin the state's Department of Social and Health Services ("DSHS") from developing an information system that would identify mental health clients and track their participation in any mental health service or public program. Id. at 931. Although the court recognized the intimate nature of the information to be stored, it held that the centralized information would be "kept strictly confidential and include no more than the patient's name and diagnostic code." Id. at 936. The fact that some DSHS individuals would have access to the raw patient data did not trouble the court; it found the system's goals "not overbroad and . . . carefully tailored to meet the State's legitimate, and laudable, interests." Id.

187. 638 F.2d 570 (3d Cir. 1980). In Westinghouse, the National Institute for Occupational Safety and Health ("NIOSH") conducted an inspection of a Westinghouse plant in Pennsylvania in reaction to a Union complaint. Id. at 572. The inspector and two NIOSH-employed physicians identified a potential health hazard, different from the one the Union complaint had alleged, and requested access to the company's medical records to examine those of the potentially exposed employees. Id. Westinghouse refused, claiming the information was protected from disclosure. Id. at 573.

188. Id. at 578. Those seven factors include:

1. the type of record requested,
2. the information it does or might contain,
3. the potential for harm in any subsequent nonconsensual disclosure,
4. the injury from disclosure to the relationship in which the record was generated,
5. the adequacy of safeguards to prevent unauthorized disclosure,
6. the degree of need for access, and
volved, the court concluded that “the strong public interest in facilitating the research and investigations of [the government agency justified] this minimal intrusion into the privacy [surrounding] the employees' medical records” and ordered Westinghouse to release the records.\textsuperscript{189} The court went on to consider whether the agency had established effective safeguards for the information so that it would be protected against subsequent unauthorized disclosure.\textsuperscript{190} The agency’s procedures for storing the records and removing the names and addresses of individuals from published reports were held to be sufficient indications of assurance of non-disclosure.\textsuperscript{191}

The duty of confidentiality regarding personal health information is also imposed under both federal and state laws.\textsuperscript{192} “Protection of the confidentiality of the medical record is the responsibility of the healthcare provider, and . . . patient authorization is usually obtained prior to disclosure.”\textsuperscript{193} The guidelines promulgated by the Joint Commission on

\begin{flushleft}
\textsuperscript{(7)} whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.
\end{flushleft}

Id.\textsuperscript{189}. \textit{Id.} at 579. Westinghouse failed to present any evidence substantiating their claim that the medical records contained highly sensitive data. \textit{Id.} According to the court, the records contained only results of routine laboratory and radiology tests which, although private, are “not generally regarded as sensitive.” \textit{Id.} Nonetheless, the court required NIOSH to give prior notice to each employee whose record NIOSH intended to review to enable the employee to raise a personal claim of privacy if so desired. \textit{Id.} at 581.

190. \textit{Id.} at 579.

191. \textit{Id.} at 580. NIOSH planned to keep excerpted data in locked cabinets inside the Medical Section of the agency during non-office hours. \textit{Id.} Further, materials used by NIOSH for small studies were not put on computers, and data from larger studies were removed from the computer after six months. \textit{Id.}

192. \textit{Institute Of Medicine}, supra note 51, at 149. Some of the laws impose the obligation on recordkeepers while others protect highly sensitive data. \textit{Id.} The Uniform Health Care Information Act (“UHIA”) of 1988 is an example of the former type of law although it has been passed in only a few states. \textit{Huffman}, supra note 167, at 582. The UHIA “prohibits a health care provider from disseminating information to a third party without the patient’s consent.” \textit{Id.} The UHIA also requires that written patient consent be obtained prior to disclosure of medical information by a health care provider at any “compulsory legal process or discovery in any judicial, legislative, or administrative proceeding.” \textit{Id.} at 583-84. Finally, the UHIA provides for access to the patient’s record by the patient. \textit{Id.} at 583.

193. Hiller, \textit{supra} note 148, at 474. Public health laws protect highly sensitive data. Many of these laws require healthcare providers “to disclose confidential medical records information without the patient’s consent” rather than to protect the records from disclosure. \textit{Roach et al.}, \textit{supra} note 2, at 86. Examples of public health laws include those

\begin{itemize}
  \item [1] that mandate reporting of actual or suspected child abuse,
  \item [2] that require physicians to identify patients receiving controlled substances,
  \item [3] that require reporting of employment-related illnesses,
  \item [4] that require reporting of abortions performed and any resulting complications,
  \item [5] that require registry of tumors,
  \item [6] that mandate informing public health authorities of infectious diseases when diagnosed,
\end{itemize}
Accreditation of Healthcare Organizations ("JCAHO"), however, are the best source of enforceable standards for the industry.\textsuperscript{194} Regardless of which standard applies, confidentiality obligations are identical for medical records kept by hand and those stored electronically.\textsuperscript{195} Perceptions of which system is more secure differ depending on the person asked. Some believe that a manual medical records system is more secure from unauthorized disclosure; others believe that electronically-stored records provide greater protection.\textsuperscript{196} Until the first CHIN becomes fully opera-

\textsuperscript{(7)} that require notification to the Nuclear Regulatory Commission any problems regarding administration of radioactive materials

\textit{Id.} at 86-90. See also Tomes, supra note 2, at 153-91.

\textsuperscript{194}. The JCAHO was formed in 1952 as an outgrowth of the American College of Surgeons. Huffman, supra note 167, at 609. From the beginning, the JCAHO "encouraged voluntary attainment of uniform high standards of care and established a structured set of standards." \textit{Id.} The JCAHO is a forerunner in the drive to shift the industry from its focus on accreditation to one on review of outcomes. \textit{Id.} at 609-10. In 1994, the JCAHO implemented the Indicator Monitoring System ("IMS") which it plans to require as a condition of accreditation of all healthcare organizations in 1996. \textit{Id.} at 610. Healthcare facilities follow a set of standards designed to define their quality of care. \textit{Id.} This data is submitted to the JCAHO which then provides comparison data back to the participating organizations. \textit{Id.} See supra note 2.


\textsuperscript{196}. Ms. Fulton warns of additional legal risks encountered when using computerized medical records, specifically the danger of too many users sharing the same information and the possibility that a single breach of security on a large centralized system might result in simultaneous disclosure of numerous records. Fulton, supra note 195, at 76-77. However well-intentioned, Ms. Fulton's concerns are anachronistic given today's technology and security systems. She also ignores the fact that manually-maintained records are physically handled by a far greater number of people during the record's life. When one healthcare provider requests a patient's medical record from another healthcare provider, at least one person must pull the record and then physically copy each page on a copier. Even if all pages are copied, they may be inadvertently misfiled or lost from either the original or the copy. The copy will then be distributed to the mail room for distribution by a messenger service or the U.S. Postal Service. If the copy is received at the requesting provider's facility, it must still be distributed to the requesting provider, going through another set or two of hands. With the exception of the caregivers in the prior scenario, none of the people handling the record have any responsibility to or relationship with the patient, but they each have access to the patient's information. See Margolis, supra note 162, at 17 (presenting the views of Dennis Dirslane, president of the healthcare division of Electronic Data Systems in Dallas, Texas).

In a recent case, an employer claimed it was entitled to an employee's prescription information in whatever form. Doe v. Southeastern Penn. Transp. Auth., 1995 WL 334290, at *7 (E.D. Pa. 1995) (unpublished opinion). The employee was HIV positive at the time of the events leading to his suit and had received a prescription for AZT, "an anti-viral drug used exclusively to treat HIV." \textit{Id.} at *2. He requested and received assurances before he filled his prescription that his name and his prescription and diagnosis could not be identi-
tional, the issue of whether the electronic medical records system is truly less secure than its manual counterpart cannot be resolved. "[T]he question is not whether computer technology will be used in the coming decade of medical practice, but rather, how and how much." 197

In planning for the inevitable electronic medical records system in which the DNA bar code is used as the unique patient identifier, every possible step to ensure confidentiality of the code and the record must be taken. The system has to be secure, yet practicable, allowing quick and easy access to records by authorized users. 198 Standard organization policies must clearly articulate the need for confidentiality and be enforced, not only against employees, but also against third parties who might have reason to access the computer. 199 The healthcare industry, with its traditions and policies, and supported by state and federal laws and regulations, is well-positioned to capitalize on technological advances that will improve quality of medical care while protecting the individual's basic privacy rights.

V. CONCLUSION: IMPLEMENTING THE PROPOSAL

The desire to understand and improve the performance of the health system begets a need for better health data. 200

---

197. Hiller, supra note 148, at 482.
198. Computer-Based Patient Records, supra note 195, at 558. Restrictive passwords are necessary to ensure that data in the system is accessed only by authorized users, but biometric means of identification would be preferred. Id. Regardless of the type of password used, the user's access should be limited to necessary information only. Id. In addition, passwords should be several characters in length and be changed frequently. Id. Logs of user access are a necessary component of any system; such logs should contain not only the date, time, and user accessing the record, but also the information that was retrieved. Id.
199. Computer-Based Patient Records, supra note 195, at 558. Software vendors and suppliers of healthcare supplies are two third-parties who might require access to a healthcare organization's system.
200. Institute Of Medicine, supra note 51, at 1.
The rapidly changing landscape of the healthcare industry as its members acquire, merge, and shift to new organizations will be the impetus for ideas designed to "improve health care delivery and to increase the value of health care spending." Using each individual's DNA fingerprint as his unique patient identifier is a radical notion, but imminently logical upon closer examination. Still, opposition to its implementation is expected. The idea will be challenged by those unwilling to adapt to the industry's new structure and by those who erroneously believe the genetic fingerprint will reveal an individual's most innermost secrets—his genetic make-up.

Cooperation among and within healthcare providers is critical to the success of the new mega-entities. "All participants in the new system . . . will need access to high quality information for informed decision making, [yet] must have confidence that information of a private nature is adequately protected." Technological innovations enable integration and multi-vendor computer systems; electronic medical records systems and CDRs, crucial to improvements in quality patient care, represent the next generation of products for the new industry. One obstacle to cooperation and information-sharing is the lack of a uniform patient identifier.

If Congress had passed the proposed Health Security Act, the country would most likely still be struggling to decide what identifier to use on the Health Security Card. Nonetheless, despite the Act's defeat in late 1994, healthcare reform continues. The quest for a uniform patient identifier continues in task forces established in federal agencies as well as within the healthcare industry itself. The social security number is an obvious choice, but has met strong opposition "because of the ease with which [it] is obtained and because of the vast amount of additional personal information accessible" through its use. One identifier not yet considered is not only unique to every individual and impossible to lose or forget, it reveals nothing about the individual or his or her personal, emotional, or financial private information: the individual's DNA fingerprint. Although the ideal choice, adopting the DNA fingerprint as the unique patient identifier will not be easy. A strategic plan that articulates clear goals and establishes realistic timeframes is required.

First, a cost-benefits analysis must be conducted to determine overall program goals and evaluate potential risks and benefits. If the trend towards community and regional healthcare networks continues, the

---

201. INSTITUTE OF MEDICINE, supra note 51, at 33.
204. Minor, supra note 8, at 253-57.
205. See supra notes 6-9 and accompanying text.
206. Minor, supra note 8, at 289.
benefits achieved by implementing this proposal will outweigh the costs. Reducing paperwork and eliminating duplicative tests are two major components of the direct savings that will occur when the DNA fingerprint identifier system is implemented. If a patient's primary provider participates in a regional or community information network, when he refers a patient to a specialist who also participates on the network, tests ordered by the primary provider will not have to be re-ordered by the specialist. The test results from the first provider, once documented in the patient's medical record, are immediately available to the specialist on the network. The patient benefits, first, by not having to submit to multiple tests, second, by not having to repeat the basis of his complaint, and third, by spending less time in the healthcare delivery system. The providers' benefits arise from savings in labor and supply costs associated with performing the tests, from requesting and transferring the patient's medical record, and from improved communications between colleagues.

Obviously, the major costs associated with this identifier system include the costs of the DNA analysis itself and the hardware, software, and network communications charges. The costs associated with performing a DNA analysis on every person who enters the healthcare delivery system appear, at first glance, to be prohibitive. However, the standard by which these costs are currently calculated is a forensic one. Moving DNA analysis into clinical and diagnostic laboratories will be initially expensive, but the increased demand for DNA profiles will reduce the per test cost significantly over time. In addition, the clinical and diagnostic laboratories must already comply with CLIA to maintain accreditation. Thus, DNA probes and profiling instrumentation that are used in a clinical and diagnostic setting will be judged by and have to conform with the same high quality control standards as any laboratory test.

Fears associated with the use of the DNA fingerprint as the unique patient identifier are without substance, but they must still be addressed. Programs for, and literature about, the DNA fingerprint must be created to dispel society's mistrust of the process and its results. The DNA fingerprint reveals no sensitive genetic information about an individual; the banding pattern that results from the profiling process is a picture of the "junk" DNA in a person's chromosomes. Scientists

207. See supra notes 105-06 and accompanying text.
208. See supra notes 100-03, 175-78 and accompanying text.
209. Much of the public's concern is a direct result of the pervasive coverage of the O.J. Simpson case in California. DNA evidence played a prominent role in the trial; expert testimony from both sides raised question after question about the quality of the process and the technicians who run the tests.
210. See supra notes 134-41 and accompanying text.
will not complete the mapping of the human genome until the year 2000 at best. Even so, knowing the location of every gene will not guarantee an understanding of the detailed nucleotide base sequence of all forty-six chromosomes; serious doubts exist about man's ability to ever create man.

Even if the banding pattern ultimately includes sensitive personal information about an individual, traditions and policies of confidentiality in the healthcare industry are well-established and are bolstered by existing state and federal laws and regulations designed to protect an individual's privacy. Further, since the profile will be used only as the individual's medical record number, the risk of using the number to access alternative data bases to gain additional personal information is minimized. No industry or government is better prepared to protect the individual from unauthorized disclosure of his DNA fingerprint than the healthcare industry.

The paradigm shift occurring in the healthcare delivery system requires a corresponding shift from traditional to creative thinking. The old healthcare provider is being replaced by larger, geographically-oriented entities. Innovative advancements in technology are being implemented, but completely achieving the ultimate goals of community-wide communications is restrained by the lack of a uniform patient identifier. This proposal to use each individual's DNA fingerprint as his unique patient identifier is revolutionary in concept, but is, nonetheless, "an idea whose time has come."

---

211. See supra note 137.
212. See supra note 137.
213. See supra notes 145-64, 179-95 and accompanying text.
214. See Minor, supra note 8, at 286-88. Unlike the social security number, the medical record number should not become a de facto standard for identification purposes. Id.