Volume 51 | Issue 4 Article 3

2006

Data Mining and Substandard Medical Practice: The Difference between Privacy, Secrets and Hidden Defects

Barry R. Furrow

Recommended Citation

Barry R. Furrow, *Data Mining and Substandard Medical Practice: The Difference between Privacy, Secrets and Hidden Defects*, 51 Vill. L. Rev. 803 (2006).
Available at: https://digitalcommons.law.villanova.edu/vlr/vol51/iss4/3

DATA MINING AND SUBSTANDARD MEDICAL PRACTICE: THE DIFFERENCE BETWEEN PRIVACY, SECRETS AND HIDDEN DEFECTS

BARRY R. FURROW*

I. INTRODUCTION

WE live in tense times. We worry about government surveillance and corporate snooping.[1] We fear misuse of our private information. We properly value privacy: it is a desirable end state and a precondition for identity, allowing individuals to achieve goals such as autonomy and solidarity with peers; it may protect the vulnerable from exposure to stigma and other harms in the larger world; it may allow us an essential space for our own thoughts and a chance to develop heretical ideas.[2] But we also know that privacy is a complex idea—that concealment of secrets by others may do us harm. At the same time, we fear that information critical to our safety will not be properly discovered and analyzed. Both the government and the private sector increasingly use "data mining"—that is, the application of database technology and techniques (such as statistical analysis and modeling) to uncover hidden patterns and subtle relationships in data, and to infer rules that allow for the prediction of future results. Many federal data mining efforts involve the use of personal information mined from databases maintained by public and private sector organizations. A recent Government Accounting Office (GAO) study found that out of 199 data mining efforts identified, 122 used personal information.[3] For these efforts, the primary purposes were detecting fraud, waste and abuse; detecting criminal activities or patterns; analyzing intelligence and detecting terrorist activities; and increasing tax compliance.[4] Most recently, a political controversy has erupted over the use by the National Security Agency of its computer capability to mine millions of email

* Professor of Law, Director, Health Law Program, Drexel University College of Law.

[1] See John Markoff, *Government Looks at Ways to Mine Databases*, N.Y. TIMES, Feb. 25, 2006, at C1 (describing new techniques used by governments to discover information about private citizens).

[2] I have discussed the broader ramifications of privacy in Barry R. Furrow, *Doctors' Dirty Little Secrets: The Dark Side of Medical Privacy*, 37 WASHBURN L.J. 283 (1998) (noting secrets kept from patients in medical context could lead to great harm to patients). For an excellent discussion of the range of privacy claims, see generally Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1088 (2002) (providing history of privacy law and advancing new, pragmatic approach to conceptualizing privacy).

[3] *See generally* GOV'T ACCOUNT OFFICE (GAO), DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES, GAO-04-548 (2004) [hereinafter DATA MINING] (summarizing various uses of data mining by government).

[4] *See id.*

messages in a search for terrorist threats.[5] Data mining is clearly a valuable tool if surrounded by proper safeguards.

The health care system unfortunately lacks systematic data collection and error reduction. The problem is not always that a provider—whether hospital, physician or clinic—is hiding poor performance as a secret. The problem more often is that flaws are buried in masses of data, hidden even from the awareness of the provider.[6] My focus is on the use of data mining of hospital patient information to better promote high quality care, particularly within the hospital setting, where most risky and invasive procedures are performed. The use of computer-generated statistical profiles of provider performance and patient outcomes is likely to move health care toward a difficult and defensive environment, at least in the near term, as providers struggle to disentangle themselves from a data web that shows them to be outliers—poor performers. Such data profiling, however, will provide hospitals with an opportunity to improve performance and will help physicians improve by recognizing their weaknesses.

I will use examples from recent staff privilege cases to examine the effects of computer programs in detecting poor quality care; evaluate the use of quality measurements and their effect on providers; and consider the implications of this move toward use of aggregate patient data through computer profiling. Such data mining and its revelations are necessary to achieve a safer and more effective health care system. In fact, providers who fail to collect data persistently using tools like data mining are, in my judgment, negligent. If properly used, the findings of data mining can focus on the essentials of performance while providing protections for physician and patient privacy. Unfortunately, the regulatory approach has too often allowed concealment of defects, at least from the prying eyes of the outside world. In a health care economy where performance matters, as measured by both positive and negative patient outcomes, we may be less tempted to tinker with the legal system to force disclosure of provider secrets.

II. THE MEANING OF PRIVACY IN THE HEALTH CARE SETTING

> Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.
>
> —*Charles Fried*[7]

[5] *See* Walter Pincus, *NSA Gave Other U.S. Agencies Information from Surveillance; Fruit of Eavesdropping Was Processed and Cross-Checked with Databases*, WASH. POST, Jan. 1, 2006, at A8 (outlining how NSA uses certain phone, fax and email records in attempts to discover terrorist connections).

[6] *See* Elizabeth A. McGlynn & Robert H. Brook, *Keeping Quality on the Policy Agenda*, 20 HEALTH AFFS. 82, 85-86 (2001) (identifying problems within health care system, specifically that data known by particular hospitals does not accurately reflect what is really happening within that hospital).

[7] Charles Fried, *Privacy*, 77 YALE L.J. 475, 475 (1968).

What are our concerns when we invoke the mantra of "privacy"? One commentator defines privacy as three related clusters of ideas: (1) physical space—"the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals"; (2) choice—"an individual's ability to make certain significant decisions without interference"; and the (3) flow of personal information—"an individual's control over the processing—i.e., the acquisition, disclosure and use—of personal information."[8] By contrast, Daniel Solove lists six characterizations of privacy values:

> (1) the right to be let alone—Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood—the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life.[9]

In light of Solove's categories, pervaded by concealment and secrets, it is clear that our uses of privacy may be less than admirable. Our definition of privacy may depend on the concealment of secrets desired by others either to protect themselves or to make their own educated choices. For example, we can manipulate others through their ignorance of our secrets, denying them knowledge that would damage our credibility if disclosed (such as a car's collision damage hidden during sale, a commercial pilot's cocaine use during flights or a person's HIV-positive status). Recasting private information as "secrets" moves our understanding toward a sense of the illicit, the impermissibly hidden. Secrets are double-edged—while we tend to view privacy as an unalloyed good,[10] we conceal to keep our secrets—and that concealment is the act of lying to others.

In the health care setting, our primary focus is on patient fears that personal information might leak out to their detriment, such as conditions that will affect their insurance, employment status or stigmatize them in some way. In addition, providers also worry about personal information that may endanger their livelihood, such as an HIV/AIDS status or sub-

[8] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-03 (1998) (outlining "three clusters" definition of privacy).

[9] Solove, *supra* note 2, at 1092.

[10] *See generally* Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964) (concluding that invasion of privacy is affront to human dignity); Charles Fried, *Privacy*, 77 YALE L.J. 475, 475 (1968) (examining right of privacy with regard to "the reasons why men feel that invasions of that right injure them in their very humanity").

stance abuse.[11] Often, privacy in health care blends information control with secrecy.

The advent of computer-based patient records, inexorable pressures to adopt linked computer systems with access to patient treatment information, and the use of the Internet to easily share information have all increased our worries about how to protect data leakage or theft. The obvious benefits of computerized record keeping have propelled medical records to a central position in health care delivery.[12] A standardized database of patient information has the potential to promote efficiency, further competition and allow providers to better track patient outcomes, so long as patient privacy interests are properly respected.[13]

Privacy rights are often little more than a grant of rights to privacy holders to control strategic secrets about themselves—secrets withheld to get someone else to act in a particular way. If the motivation for hiding information is to deceive, then privacy protects fraud. Is there any good reason to let people have property rights in secret information about themselves that will discredit them if revealed?[14] In the abstract, the answer is clearly no. In the medical environment, the guiding principle should be discovery of "secrets" and harvesting of data regarding defects in the system. Ultimately, concealment in medicine can do great harm to patients.

A. *Information Control*

Control over our information and its dissemination to others is of most interest to me in the context of medical errors and patient injury. President Clinton's Information Infrastructure Task Force has defined privacy as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed and used."[15] The Supreme Court has stated that privacy is "control over information concerning his or her person."[16] Such definitions beg

[11] *See generally* Doe v. Medlantic Health Care Group, Inc., 814 A.2d 939 (D.C. 2003) (discussing suit for breach of confidentiality by hospital for revealing patient's AIDS status).

[12] *See generally* Nicholas P. Terry, *To HIPAA, a Son: Assessing the Technical, Conceptual, and Legal Frameworks for Patient Safety Information,* 12 WIDENER L. REV. 137 (2005) (highlighting impact of technology on patient information).

[13] It is also clear that we have a long way to go to incorporate electronic records and computerized systems in the complex health care enterprise.

[14] *See* INST. OF MED., HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY (M.S. Donaldson and K.N. Lohr eds., 1994); OFFICE OF TECH. ASSESSMENT, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION, OTA-TCT-576 (1993) (presenting report examining problems relating to health care privacy, curative proposals and privacy models); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform,* 48 VAND. L. REV. 295, 306-09 (detailing privacy concerns within health care sector).

[15] CLINTON'S INFO. INFRASTRUCTURE TASK FORCE (IITF): PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 5 (1995).

[16] U.S. Dep't of Justice v. Reporters Comm., 489 U.S. 749, 763 (1989).

the harder question: to what extent do health care providers and health care institutions have privacy rights to control information that may prove damaging to them?[17] Privacy cannot be simply a claim that an individual can decide what information about himself or herself may be disclosed. Privacy in the form of secrets may in fact violate moral principles of avoiding harm to others. The parameters of a definition of privacy rights also concern what society decides is deserving of protection.

Privacy protections serve important functions in our society. But while health care providers such as physicians and nurses deserve privacy as citizens, their power over patients as providers exposes potential risks. Medical secrecy therefore deserves close scrutiny as a protected right. We have long been worried about patient information and its possible leakage into the wrong hands—blackmailers, thieves or simply marketing profilers who disclose their information to businesses seeking either to find new customers, or to avoid problematic ones. Such leakage and resulting damage have occurred in the past simply because of the porosity of hospitals and their frequent inability to protect vulnerable patient information.

We also know that physicians may lie about their secrets, such as substance abuse problems, failing vision, depression and slipping performances. Here we typically trust the institutions in which they work, primarily hospitals, to police their secrets, ferret them out and take appropriate action without requiring a physician to stigmatize herself or himself by disclosing personal problems to patients.[18] As an illustration, consider the physician in *Semeraro v. Connolly.*[19] In the case, the plaintiff was referred to Dr. Connolly, a specialist in colorectal cancer, for testing of her colon. While performing a colonoscopy, Dr. Connolly discovered a polyp growth on her colon, which was then promptly removed. Subsequently, he was unable to determine if the polyp was completely removed, due to poor preparation of her colon area. Six years later, during the plaintiff's examination by another colorectal cancer specialist, a large polyp growth and tumor on her colon had to be removed.

[17] *See, e.g.*, Ian Goldberg et al., *Trust, Ethics, and Privacy*, 81 B.U. L. REV. 407, 418 (2001) ("We build our own definition of privacy on what we consider the most elegant definition, 'informational self-determination,' which refers to a person's ability to control the flow of his own personal information."). In their famous article on the right to privacy use and the language of information control, Warren and Brandeis stated:

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. . . . [E]ven if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

[18] *See* Furrow, *supra* note 2, at 291-96 (outlining reasons for not mandating physician disclosure to patients of their personal flaws).

[19] No. CIV.A.92-4636, 1992 WL 392621 (E.D. Pa. Dec. 14, 1992).

After her initial treatment with Dr. Connolly, the plaintiff discovered that Dr. Connolly retired from the practice of medicine in 1987 due to the "deterioration of his sight, coordination and mental facilities."[20] Eventually, he was diagnosed with Alzheimer's disease and died in 1990. Plaintiff sued, arguing that Dr. Connolly failed to reveal the deterioration of his skills to her in 1984 or any time thereafter, and that if she had been notified of his condition she would have refused treatment. She also proposed a duty of disclosure at the time of Dr. Connolly's retirement to all patients. The court held that the informed consent doctrine "does not allow recovery for failure to reveal information pertaining to the personal characteristics of the physician."[21] Quoting from an earlier case rejecting disclosure of a physician's alcoholism,[22] the court stated:

> Matters such as personal weaknesses and professional credentials of those who provide health care are the responsibility of the hospitals employing them, the professional corporations who offer their services, or the associations that are charged with oversight. Their failure to fulfill their obligations in this regard becomes a matter of negligence, and it is from them that recovery must be sought.[23]

We want our institutions to have the tools, and the willingness to use them, to determine which providers pose risks to patients. Therefore, it is the information gathered and stored by hospitals that is most central to patient safety, and it should be the least protected by privacy principles.

B. *Defect Detection in Institutions*

Concerns about the privacy of patient medical information have intensified with the growth of both electronic record keeping and the Internet. The federal government studied this problem for several years before developing a highly detailed set of standards for health care providers. The Medical Privacy Standard of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[24] was drafted and implemented to create a new range of patient rights, protecting their medical information in light of the implementation of the patient electronic medical record. The Medical Privacy rules of HIPAA offer a "minimum necessary" rule to disclosure and use of patient information.[25] HIPAA has moved the focus

[20] *Id.* at *2.

[21] *Id.*

[22] *See generally* Kaskie v. Wright, 589 A.2d 213 (Pa. Super. Ct. 1991) (rejecting claim that physician's alcoholism should have been disclosed, along with absence of license to practice in Pennsylvania).

[23] *Id.* at 217.

[24] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (proposed Dec. 28, 2000) (codified at 45 C.F.R. pts. 160 and 164).

[25] *See* James G. Hodge, *The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Workers' Compen-*

of medical privacy toward the institution, limiting its disclosures and discussions. It has moved medical records privacy beyond the current rigid common law approach that places the responsibility on physicians.[26] Although HIPAA offers incomplete patient protection, it has made medical record keeping and patient information a central and regulated aspect of hospital practice. In addition, as part of the larger regulatory effort to promote the electronic patient record, HIPAA provides a fertile underpinning for data mining of medical errors and problems that develop.

Control over information as an aspect of privacy is only part of the problem in the health care setting. The harder questions stem from how such information is collected, processed and used. The very value of this information is that it is aggregated, subjected to a bureaucratic process that can have built-in protections, and the individual provider informed how the information is processed and used. We move beyond privacy concerns to those of institutional due process under staff privilege by-laws and other safeguards.[27]

Medical secrets fall into three categories: patient medical secrets, physician secrets and organizational secrets. The patient may fear revelation of his secrets to a health care provider—nurse, physician or hospital—because they may be rebroadcast by physicians to staff and then on to the outside world.[28] Or the patient may fear that instead of a sloppy rebroadcast, a pointed inquiry by a particular third party will disclose the information and intrude into the seclusion so carefully constructed.[29] Health care providers are notoriously porous vessels, revealing patient confidential information at alarming rates. Medical record privacy is a current concern for patients in light of the pressure for more information, computer link-

sation, 51 ADMIN. L. REV. 117, 127-36 (1999) (describing various aspects of HIPAA as relating to medical privacy); INST. FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIV., HEALTH PRIVACY PROJECT, THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN (July 1999), http://www.healthprivacy.org (discussing current problems with privacy in health care sector).

[26] *See* Terry, *supra* note 12, at 405 (arguing "the institutional provider will become the default defendant in informed consent cases").

[27] *See* Solove, *supra* note 2, at 1154 (moving towards due process model with respect to privacy concerns instead of standard privacy law).

[28] *See generally* Doe v. Marselle, 675 A.2d 835 (Conn. 1996) (discussing disclosure of plaintiff's HIV-positive status by employee of surgeon); Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451 (1995) (discussing privacy in health care sector generally with focus on why patients might not want their information revealed); Lawrence O. Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, 5 HEALTH MATRIX 1 (1995) (same).

[29] *See generally* Judice v. Hosp. Serv. Dist. No. 1, 919 F. Supp. 978 (E.D. La. 1996) (presenting situation where neurosurgeon was recovering alcoholic); McDaniel v. Miss. Baptist Med. Ctr., 877 F. Supp. 321 (S.D. Miss. 1995) (determining whether medical center employee terminated due to drug use violated ADA); Altman v. N.Y.C. Health & Hosps. Corp., 903 F. Supp. 503 (S.D.N.Y. 1995) (presenting situation where physician was recovering alcoholic).

ages of computerized patient files for insurance and other purposes.[30] HIPAA's Medical Privacy Standards are a compromise approach to this problem, granting some privacy rights while limiting remedies for curing breaches of privacy.

Institutions that we depend on for goods and services may have secrets, information that if released would cause us to avoid their goods and services, criticize them or take other steps damaging to them. Given their complexity, institutions may be toxic, producing harm without awareness. They may also have hidden flaws, undiscovered perils lurking within their operating environment—accidents about to happen, workers on the edge, flaws that have yet to materialize—in other words, as yet undiscovered risks. These defects are not secrets, because they are not known and therefore concealed. Rather, they are buried defects, concealed in masses of unanalyzed data, with possible patterns simply not detected by the institutions.

Such patterns can be uncovered by computer data mining. Here, my concern is specifically hidden sources of bad patient outcomes or substandard performance generally in the hospital setting. Undiscovered sources of provider error, system failures and harm to patients may be even more deadly. They are not secrets in a sense because the provider is not concealing information it already knows and is worried about disseminating. Rather, the knowledge is more like a hidden flaw that must be uncovered and extirpated before more damage is done. Like a stress line in a metal tool or an aneurysm in someone's brain, these flaws are increasingly discoverable within health care institutions. And if discovered, they can often be fixed. The solutions may include staff or hospital actions against a toxic physician, a repair to a flawed system of medication delivery, medical device procurement or an improved computer entry system. But solutions are not possible unless the hidden flaw is discovered. The tools of outcome measurement and data mining provide powerful tools for such discovery.[31]

III. MEDICAL ERRORS: CONCEALED FLAWS

> It may seem a strange principle to enunciate as the very first requirement in a Hospital that it should do the sick no harm.
>
> —*Florence Nightingale*[32]

Patients suffer unnecessary injuries and death at the hands of health care providers, both because they receive substandard care and because

[30] *See* Gostin, *Health Information Privacy, supra* note 28, at 454 (stating "protecting the confidentiality of medical records is an absolutely essential or very important part of national health care reform").

[31] *See generally* Gary T. Marx & Nancy Reichman, *Routinizing the Discovery of Secrets: Computers As Informants*, 27 AM. BEHAV. SCIENTIST 423 (1984) (discussing problems with data mining broadly in civil liberties context).

[32] FLORENCE NIGHTINGALE, NOTES ON HOSPITALS (1859).

they fail to get necessary and effective treatments.[33] The Institute of Medicine's 1999 projection of up to 98,000 deaths per year,[34] and hundreds of thousands of avoidable injuries and extra days of hospitalization,[35] has been enlarged by analyses that are more recent. A HealthGrades analysis of Medicare data projected a casualty rate almost twice the Institute of Medicine figures, or 195,000 deaths per year attributable to adverse medical events.[36] The Centers for Disease Control has estimated that medical errors, if ranked as a disease, would be the sixth leading cause of death in the United States, outranking deaths due to diabetes, influenza and pneumonia, Alzheimer's disease and renal disease.[37] Others rank health care, more generally defined, as the third leading cause of death in this country.[38] Increasingly, Medicare patients are experiencing a high level of errors.[39] For example, patient infection studies have found astonishing levels of preventable and often deadly infections.[40] Further, "[h]ospital-acquired infections rates worsened by approximately 20% from 2000 to 2003 and accounted for 9,552 deaths and $2.60 billion, almost 30% of the total excess cost related to the patient safety incidents."[41] Moreover, unnecessary surgery, by one estimate, kills over 12,000 people each year.[42]

[33] I treat this issue of medical error and patient safety, seen as a broad regulatory problem, in Barry R. Furrow, *Regulating Patient Safety: Toward Federal Model of Medical Error Reduction*, 12 WIDENER L. REV. 1 (2005).

[34] This projection has been criticized as based on a methodology that is likely to overstate the death rate. *See* Rodney A. Hayward & Timothy P. Hofer, *Estimating Hospital Deaths Due to Medical Errors: Preventability Is in the Eye of the Reviewer*, 286 JAMA 415, 415-20 (2001) (examining reliability of reviewers as cause for overstatement of death rate).

[35] *See* COMM. ON QUALITY OF HEALTH CARE IN AM., INST. OF MED., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM (L.T. Kohn, J.M. Corrigan & M.S. Donaldson eds., Nat'l Academy Press 2000) [hereinafter "IOM REPORT"].

[36] *See* HEALTHGRADES, INC., SECOND ANNUAL PATIENT SAFETY IN AMERICAN HOSPITALS REPORT (2005) (presenting and analyzing multitude of statistics outlining problems with patient deaths in hospitals).

[37] *See* Nat'l Vital Statistics Report, *Deaths: Preliminary Data for 2002* Vol. 52, No. 13 (Kenneth D Kochanek & Betty L. Smith eds., 2004) (analyzing cause of death data and statistics, including data concerning hospital errors).

[38] *See* Bruce Spitz & John Abramson, *When Health Policy Is the Problem: A Report from the Field*, 30 J. HEALTH POL. POL'Y & L. 326, 329 (2005) (providing statistics regarding health care as cause of death).

[39] *See* MEDICARE PAYMENT ADVISORY COMM'N, REPORT TO CONGRESS: MEDICARE PAYMENT POLICY (2005) (noting problems with current Medicare system and advocating pay-for-performance method of payment to insure higher quality performance by hospitals and physicians).

[40] *See id.* (offering example of medical error).

[41] HEALTHGRADES, *supra* note 36, at 3.

[42] *See* Barbara Starfield, *Is U.S. Health Care Really the Best in the World?*, 284 JAMA 483, 483 (2000) (noting unnecessary surgery as cause of high number of deaths).

The accumulating data on patient injury continues to startle any outside observer.[43] At least three to four percent of all hospitalizations give rise to adverse events.[44] Provider-caused injury is a predictable feature of hospital care.[45] American medicine creates too much patient harm, in spite of its technological prowess.[46] Moreover, much of this harm is concealed—buried under a mass of data in complex and often chaotic health care institutions.[47] Mining medical error data is crucial for reducing the volume of medical adverse events suffered by patients in American hospitals.[48]

[43] The Agency for Healthcare Research and Quality (AHRQ) recently developed and released a set of Patient Safety Indicators (PSIs) specifically designed for screening administrative data for incidences of concern related to patient safety. AHRQ is the lead agency for the U.S. government on quality in health care, sponsoring research that examines the frequency and cause of medical errors and testing techniques designed to reduce these mistakes. Using this measurement tool, AHRQ identified the rates of, and excess length of stay and mortality associated with, these specific patient safety indicators. Extrapolating from AHRQ's sample data, representing approximately twenty percent of all U.S. hospitals (2000 Healthcare Cost and Utilization Project Nationwide Inpatient Sample), researchers estimated that the eighteen patient safety indicators evaluated contributed to $9.3 billion excess charges and 32,591 deaths in the United States annually. *See* HEALTHGRADES, INC., FIRST ANNUAL PATIENT SAFETY IN AMERICAN HOSPITALS REPORT (July 2004), http://www.healthgrades.com/media/english/pdf/HG_Patient_Safety_Study_Final.pdf; AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, PATIENT SAFETY INDICATORS (Feb. 2006), http://www.qualityindicators.ahrq.gov/psi_overview.htm; *see also* Bryan J. Weiner et al., *Quality Improvement Implementation and Hospital Performance on Patient Safety Indicators,* 63 MED. CARE RES. & REV. 29 (2006).

[44] *See* T.A. Brennan et al., *Incidence of Adverse Events and Negligence in Hospitalized Patients: Results of the Harvard Medical Practice Study I,* 13 QUAL. & SAF. HEALTH CARE 145 (2004).

[45] *See* David M. Studdert et al., *Beyond Dead Reckoning: Measures of Medical Injury Burden, Malpractice Litigation, and Alternative Compensation Models from Utah and Colorado,* 33 IND. L. REV. 1643, 1662 (2000) (noting high predictability of medical mishaps caused by hospitals and doctors). The Utah-Colorado Medical Practice Study (UCMPS) found that adverse events connected to surgery accounted for about half (44.9%) of adverse events across both states, with only 16.9% of the surgical adverse events involving negligence. The authors concluded that the UCMPS produced results similar to the earlier New York Harvard Study. *Id.*

[46] *See* Mark R. Chassin et al., *The Urgent Need to Improve Health Care Quality,* 280 JAMA 1000, 1001 (1996) (highlighting various serious problems within United States health care system).

[47] One patient survey found that nearly twenty-two percent of patients had experienced a medical error, with preventable adverse drug events the largest contributor to these errors, leading the Fund to project a much higher rate of patient injury caused by medical errors and drug adverse events. *See* SHEILA LEATHERMAN & DOUGLAS MCCARTHY, THE COMMONWEALTH FUND, QUALITY OF HEALTH CARE IN THE UNITED STATES: A CHARTBOOK 64 (2002) (discussing serious problem of physicians administering incorrect drugs to patients, leading to deaths).

[48] *See generally* Lucian L. Leape, *Reporting of Adverse Events,* 347 NEW ENG. J. MED. 1633 (2002) (emphasizing importance of mining medical data for protection of patients).

A. *Quality Assurance and Outcome Measurement*

Modern computers allow sensitive health care data to be stored, transferred and used with ease. Given the sheer volume of data collected on each patient, the movement to computerize patient records has been pushed by pressures from the federal and state governments as well as hospitals' desires for efficiency. As health care has blossomed into a complex industry, the organizations involved—from employers to drug companies and managed organizations—have a compelling interest in data to control their costs, increase revenues and improve performance. Information has, as a result, become a central aspect of the health care enterprise.[49] For example, the American College of Surgeons has developed the National Surgical Quality Improvement Program (ACS NSQIP), the first nationally validated, risk-adjusted, outcomes-based program to measure and improve the quality of surgical care.[50] Concerns about medical record privacy have grown as storage of digital information has become more common.[51]

[49] *See* COMM. ON MAINTAINING PRIVACY & SEC. IN HEALTH CARE APPLICATIONS OF THE NAT'L INFO. INFRASTRUCTURE, NAT'L RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 25 (1997) (noting that more than half of hospitals were investing in electronic medical records and market was expected to grow into $1.5 billion industry by 2000); Gostin, *Health Information Privacy*, *supra* note 28, at 452 (stating that high quality information is necessary for informed decision-making); Paul Starr, *Health and the Right to Privacy*, 25 AM. J.L. & MED. 193, 196 (1999) (discussing importance of health care data and information). *See generally* David M. Studdert, *Direct Contracts, Data Sharing and Employee Risk Selection: New Stakes for Patient Privacy in Tomorrow's Health Insurance Markets*, 25 AM. J.L. & MED. 233 (1999) (describing potential problems regarding increased access to health information).

[50] *See* AM. COLL. OF SURGEONS, CONTINUOUS QUALITY IMPROVEMENT: ACS OUTCOMES DATABASES, http://www.facs.org/cqi/outcomes.html (last visited Apr. 22, 2006) (providing general overview of ACS NSQIP).

[51] Violations of health information privacy fall into three major categories. The first is abuse or misappropriated medical record information. For example, the increased use of e-mail messages from patients to their physicians can lead to the storage of these messages in the file, allowing the patient's own words to be easily accessed. Patients may reveal too much in light of the casual and conversational attributes of e-mail messaging. Hackers may also gain access to hospital medical record systems. Data security measures and sanctions against misuse can reduce this problem. Second, health information may be used by institutions for marketing and other commercial purposes. For example, the health care institution may sell patient prescription information to direct mail companies. Third, organizations may abuse confidential patient health information in substantial and serious ways that result in discrimination, loss of employment, insurance or other welfare benefits. *See* Alissa R. Spielberg, *Online Without a Net: Physician–Patient Communication by Electronic Mail*, 25 AM. J.L. & MED. 267, 274 (1999) (describing how physicians currently handle e-mail communications with clients and pitfalls regarding use of e-mail); Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L. MED. & ETHICS 98 (1997). *See generally* OFFICE OF TECH. ASSESSMENT, U.S. CONG., POLICY IMPLICATIONS OF MEDICAL INFORMATION SYSTEMS 50–51 (1997); OFFICE OF TECH. ASSESSMENT, U.S. CONG., PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION 11-12 (1993) (describing some pitfalls regarding accumulation of medical data); Janlori Goldman, *Protecting Privacy to Im-*

The evolution of quality assurance in health care entities has moved toward continuous quality improvement, a method of constantly evaluating and changing health care with quality parameters in mind.[52] Continuous quality improvement requires a focus on comparative data as to effectiveness of medical procedures, feedback and education of physicians and development of practice guidelines that embody the research findings. Hospitals and managed care organizations actively engage in programs to promote high quality and effective practice, through implementation of clinical algorithms, outcome based studies, application of quality control principles from industry and large-scale analysis of practice patterns across plans. These programs of outcome management are now being implemented in hospitals and managed care organizations under pressure from the hospital accrediting body—the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)—and the federal government.[53]

This change in focus within health care institutions toward quality improvement has been expedited by the rapid acceleration of information gathering by health care institutions. Such information gathering by health care institutions is likely to have two legal effects. First, it will lead to demands for disclosure of such comparative success rates and outcome data where available.[54] Current regulatory strategies are driven by the idea of patients as consumers, and the value of quality information and comparative data to both patients and payers as they evaluate care. Reporting of adverse events and near misses is an essential part of an information infrastructure.[55] The candidates for data reporting and public

prove Health Care, 17 HEALTH AFFS. 47 (1998) (detailing recent events that have increased public's fear about misuse of medical data, including two instances where pharmacies disclosed patient's prescription information to direct mail services and pharmaceutical companies); John D. Rootenberg, *Computer-Based Patient Records: The Next Generation of Medicine?,* 267 JAMA 168, 168 (1992) (discussing advantages that result from using only computer-based patient records and doing away with handwritten charts); INST. OF MED., THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE (1997), http://www.nap.edu/readingroom/.

[52] *See generally* CONTINUOUS QUALITY IMPROVEMENT IN HEALTH CARE: THEORY, IMPLEMENTATIONS, AND APPLICATIONS 3-33 (Curtis P. McLaughlin & Arnold D. Kaluzny eds., 3d ed. 2006) (1999) (defining continuous quality improvement and listing many characteristics of continuous quality improvement program).

[53] *See* Solove, *supra* note 2, at 1090.

[54] *See generally* Paul D. Rheingold, *The Admissibility of Evidence in Malpractice Cases: The Performance Records of Practitioners,* 58 BROOK. L. REV. 75, 80 (1992) ("It does seem inescapable . . . that part of the information about risks would be what the doctor's own experience has been, even if all risks are lumped together."); Aaron D. Twerksi & Neil B. Cohen, *Comparing Medical Providers: A First Look at the New Era of Medical Statistics,* 58 BROOK. L. REV. 5, 12-13 (1992) (predicting that as statistical validity of data is established, it will become part of litigation).

[55] *See* Elizabeth A. McGlynn & Robert H. Brook, *Keeping Quality on the Policy Agenda,* 20 HEALTH AFFS. 82, 86 (2001) (stating what authors believe are essential requirements of effective information system).

availability are many. One example is infection control report cards.[56] It may be that a graphic depiction of a hospital's progress over time is more useful than cross-institution comparisons.[57] Generating the reports in a graphic way so that hospital providers can clearly see baselines and improvement is a goal worth mandating. The goal of data transparency, however, may be valuable as much for internal learning and staff privileging decisions as for consumer and buyer shopping, at least in the short-term.[58]

The push toward electronic records and data gathering may also change the standard of care for hospitals, leading to the use of data mining as a standard operating procedure. Comparative outcome data ultimately raises the possibility that such data must be gathered, evaluated and used by hospitals and managed care organizations to reduce the risk of harm to patients.

B. *Data Mining*

The idea of systematically collecting and studying information of all kinds on patient progress through a health care institution is not new. Dr. Ernst Codman was one of the first to advocate a hardheaded approach to data collection and error reduction.[59] Codman was a Boston doctor who wanted hospitals and doctors to track their practices and evaluate outcomes of their patients, an ideal he developed around 1920.[60] He offered an "end-result system" based "'on the common-sense notion that every

[56] *See generally* Robert A. Weinstein et al., *Infection-Control Report Cards—Securing Patient Safety*, 353 NEW ENG. J. MED. 225 (2005) (suggesting that report cards are important tool in analyzing health care providers).

[57] *See id.*

> We have also learned that we must select denominators carefully in order to avoid artificial inflation or deflation of rates; that sophisticated information technology is required; and that it can be difficult to define useful benchmarks, . . . so that reporting a trend for a particular hospital may provide more useful information than does comparing hospitals.

Id.

[58] *See* Ashish K. Jha et al., *Care in U.S. Hospitals—The Hospital Quality Alliance Program*, 353 NEW ENG. J. MED. 265, 272 (2005).

> Our findings indicate that quality measures had only moderate predictive ability across the three conditions. Although a high quality of care for acute myocardial infarction predicted a high quality of care for congestive heart failure, the former was only marginally better than chance at identifying a high quality of care for pneumonia. These data do not provide support for the notion that "good" hospitals are easy to identify or consistent in their performance across conditions. Our data suggest that evaluations of hospitals' performance will most likely need to be based on a large number of conditions.

Id.

[59] *See generally* Susan Reverby, *Stealing the Golden Eggs: Ernest Amory Codman and the Science and Management of Medicine*, 55 BULL. HIST. OF MED. 156 (1981) (describing Dr. Ernst Codman's efforts to link standardized clinical care with hospital reform).

[60] *See id.* at 168-69 (describing early attempts at hospital standardization).

hospital should follow *every* patient that it treats, long enough to determine whether or not the treatment has been successful, and then to inquire 'if not, why not?' with a view to preventing similar failures in the future.'"[61]

Codman's central idea was a complete patient record that included assessments of why a treatment was unsuccessful—including discussion of errors of technical knowledge or risk, lack of surgical judgment, lack of care or equipment, lack of diagnostic skill, unconquerable disease, patient's refusal of treatment, calamities of surgery or accidents and complications over which doctors had no control.[62] This detailed record was to serve an auditing function to evaluate, compare and establish benchmarks for the performance of physicians and hospitals. Codman was ahead of his time, hoping to assess a hospital's efficiency in therapeutic, outcome-based terms. To Codman, patient harm due to infections or unnecessary or inappropriate operations was a hospital "waste product."[63] His analogy of bad outcomes to waste products was brilliant.[64] Data mining is different from Codman's idea of systematically tracking each patient's progress explicitly through a health care system, a process that hospitals attempt to varying degrees of success. Data mining, by contrast, is a computerized hunt for patterns and causes; it is the process of automatic systematic searching for patterns in large quantities of data.[65] It is a problem-solving tool that analyzes existing data in large databases, through patterns represented in structures, patterns or clusters that can be used to inform future decisions.[66] It extracts predictive information from these large databases, finding hidden patterns that may lie outside viewer expectations or be invisible on a case-by-case basis.[67] It is focused on hypothesis generation,

[61] VIRGINIA A. SHARPE & ALAN I. FADEN, MEDICAL HARM: HISTORICAL, CONCEPTUAL, AND ETHICAL DIMENSIONS OF IATROGENIC ILLNESS 29 (1998) (quoting Dr. Ernst Codman). *See generally* Reverby, *supra* note 59 (detailing life and work of Dr. Ernst Codman).

[62] *See* Reverby, *supra* note 59, at 156.

[63] *See* SHARPE & FADEN, *supra* note 61, at 31 (defining way Codman characterized things that could prevent unnecessary patient death).

[64] Codman's work eventually led to the Joint Commission on Accreditation of Health Care Organizations (JCAHO), which has slowly moved toward a more outcome-based accreditation system.

[65] Data mining lacks a precise meaning, because it includes a range of analytic activities, including data profiling, data warehousing, online analytical processing and enterprise analytical applications. Other terms used include "factual data analysis" and "predictive analytics." The generally accepted definition is "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results." DATA MINING, *supra* note 3, at 1 (explaining how "data mining" was defined for purposes of study).

[66] *See* IAN H. WITTEN & EIBE FRANK, DATA MINING: PRACTICAL MACHINE LEARNING TOOLS AND TECHNIQUES 5 (2d ed. 2005) (explaining how data mining works and how it is utilized).

[67] *See* D. Kopec et al., *Human Errors in Medical Practice: Systematic Classification and Reduction with Automated Information Systems* (Oct. 15, 2002), http://www.sci.

not hypothesis testing (which may lead to missed associations).[68] This approach is especially appropriate for medical data, which often exists in vast quantities in an unstructured format. Applying data mining techniques can facilitate systematic analysis.

Data mining uses specialized software tools based on advanced search algorithms, multiprocessor computers and massive databases to discover knowledge that is often unexpected. Companies, such as IBM, with its DB2 Intelligent Miner,[69] ACS's MIDAS+ Comparative Performance Measure System[70] and SPSS Inc.'s data mining software,[71] provide software products to health care companies to allow them to mine large volumes of data and harvest risk-related results and outcome comparisons.[72]

Data mining can solve a range of tasks.[73] These may include: (1) predicting—learning a pattern from examples and using the model to predict future values of the target variable; (2) classification—finding a function that groups records into discrete classes; (3) detection of relations—searching for the independent variables for a selected target of variables; (4) explicit modeling—finding explicit formulae describing dependencies between various variables; (5) clustering—identifying groups of records that are similar between themselves but different from the rest of the data; and (6) deviation detection—determining the most significant changes in some key measures of data from previous or expected values.

Data mining is therefore a powerful new addition to outcomes measurement, moving beyond tracking a particular patient to a satellite view of the whole population of a hospital over time. Using pattern recognition

brooklyn.cuny.edu/~kopec/research/new/Final_J_Med_Sys_10_16_02.pdf (describing use of automated systems to reduce human medical errors).

[68] *See* John H. Holmes, *Mining Health-Related Data: Methods and Applications in Research, Public Health, and Patient Care* 14, http://infranet.uwaterloo.ca/inftalks/2003-2004/2003-10-22/default.pdf (last visited Apr. 22, 2006) (reiterating focus of data mining).

[69] *See* IBM Software, DB2 Intelligent Miner, http://www.306.ibm.com/software/data/iminer (last visited Apr. 22, 2006) (providing information about IBM's DB2 Intelligent Miner software).

[70] *See* Affiliated Computer Services, *The MIDAS+ Comparative Performance Measurement System: A Core Measure Solution,* http://www.midasplus.com/cpmsfea1.html (last visited Apr. 22, 2006) (describing program and features of MIDAS+ data mining software).

[71] *See* SPSS, *Healthcare: Ensuring Quality of Care,* http://www.spss.com/vertical_markets/healthcare/quality.htm (last visited Apr. 22, 2006) (providing information about SPSS's data mining software).

[72] *See* SPSS, *Customers: San Francisco Heart Institute,* http://www.spss.com/success/template_view.cfm?Story_ID=38 (last visited Apr. 22, 2006) (profiling San Francisco Heart Institute's use of SPSS software). The Institute collects data to evaluate patient risk, effectiveness of procedures and medications and physician performance. *Id.*

[73] *See* Megaputer Intelligence, *What Is Data Mining?*, http://www.megaputer.com/dm/dm101.php3 (last visited Apr. 22, 2006) (describing PolyAnalyst as one commercially available program for data mining that advertises that it can perform all functions listed).

algorithms, data mining can be set to search databases to investigate particular problems. It can spot trends in infections using infection surveillance results. Alternatively, it can be used in a broader way to mine for hidden problems, trends or other patterns that are fixable. IBM cites the benefits of its DB2 Intelligent Miner, using as an example a Florida Hospital where data miners found that pneumonia patients who were not given medication immediately upon admittance suffered significantly worse outcomes than those who were.[74] At another facility, data mining showed that patients with cardiovascular disease were not always prescribed beta-blockers because the discharge process did not include a crucial step to ensure the prescription was ordered, and that an easy solution was to change work processes.

IV. THE LIMITS OF PROVIDER PRIVACY: OUTLIERS, DETECTABLE PATTERNS AND HARM

> [S]ecrets are also used as tools of power, wrenching advantage from the unknowing actions of others. What we do not know often *does* hurt us—and serves to benefit others who kept us in the dark. Secrets provide the unobservable weapons of the devious.
>
> —*Kim Lane Scheppele*[75]

Pure provider secrets may conceal treatment risks from patients. Such secrets include information that a patient might like to know about an individual physician in order to protect himself from harm at the hands of that physician—a physician's alcoholism, mental or physical deterioration, contagious disease status and most important, his or her performance limitations.[76] Some private information may not be directly relevant to patient risk, but its disclosure may stigmatize or otherwise damage the health care provider.[77] Hospitals can detect some provider problems dur-

[74] *See* Alex Veltsos, *Getting to the Bottom of Hospital Finances: Florida Hospital, an Experienced Data Miner, Stretches Its Extensive Use of Data Mining to Deliver Financial Results That Will Improve Its Bottom Line—Data Warehousing/Mining*, HEALTH MGMT. TECH. (Aug. 2003), http://www.findarticles.com/p/articles/mi_m0DUD/is_8_24/ai_106474733 (providing first-hand description of Florida Hospital's use of IBM's data mining software to improve hospital).

[75] KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 5 (1988).

[76] *See generally* Doe v. Marselle, 675 A.2d 835 (Conn. 1996) (describing situation where patient's HIV-positive status was disclosed to members of community by employee of surgeon); Gostin, *Health Information Privacy*, *supra* note 28 (describing information that patients need in order to make informed decision about physicians); Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, *supra* note 28; Schwartz, *supra* note 14, at 301 (explaining that there is widening audience of outside observers now watching performances of doctors, nurses and patients).

[77] Disclosure of a physician's physical condition—for example, an addiction like alcoholism—raises troubling legal issues. Certainly, an alcoholic surgeon may

ing credentialing of physicians; other problems may not be detected, or may develop later on.

Perhaps more important are the undiscovered sources of patient harm—the connections, system processes or provider missteps that create risks to patients. These flaws—the risks and near misses—are not secrets, not yet, since secrecy implies information that is concealed; they are instead un-mined and therefore undiscovered ore. To what extent does a provider owe a patient a duty not only to reveal and fix dangerous secrets within his or her walls, but also to affirmatively mine his or her data relentlessly to ensure that other sources of patient harm do not exist, or are detected and fixed? The standard of practice should reflect an obligation to discover sources of human error and patterns of harm creation with the goal of reducing and eliminating them.

I leave to others the protection of patient information. Neither individual providers nor organizations should have the kind of expectations of privacy that patients are owed. Providers' privacy expectations should not include performance limitations that may harm patients. What attracts me about the proper use of data mining is its ability to spot patterns, trends and comparative effects in a visual way, without the need to dig into the patients' records in a hunt for gold, or into the physician's personal limitations in ways that may invade her privacy while being irrelevant to performance.[78]

A. *Institutional Responsibility for Patterns*

1. *Staff Privileging Actions*

Data mining, as a subset of outcome measurement generally, may reveal patterns of substandard care. The fairest use of this information is at the level of the institutional provider. The role of the institution and peers in controlling these practices is central to reducing the risks, backstopped by the ever-present threat of a tort suit for damages. Hospital medical staff tort law has focused on provider competency in articulating the limits of negligent staff selection. Hospitals screen their medical staff to reduce the level of risk of injury to their patient population, refusing to credential high-risk physicians. Risk is defined by a competency/quality definition. The standard is skills-based—assuming that a low level of skill creates unnecessary risks to the patient—and outcome-based—looking to impairments or other physician limitations that might increase risks to patients. Hospital staff privilege disputes increasingly reveal flaws within a hospital that are detected by the use of computer analyses that spot

have an impairment that might seriously affect performance and thus success rate. *See* Kaskie v. Wright, 589 A.2d 213, 217 (Pa. Super. Ct. 1991) (rejecting claim that physician's alcoholism should have been disclosed, along with absence of license to practice in Pennsylvania).

[78] *See id.* at 213-17 (same).

problems. Hospitals may then take steps to reduce patient harm based on the data.

One example is the case of *Unnamed Physician v. Board of Trustees of Saint Agnes Medical Center.*[79] The hospital had used a Midas data mining program as a part of the reappointment process, and the program generated a statistical analysis of outliers in the hospital physician's performance, including infection rates flagging the outlier physicians.[80] For the period from January 1, 1999 to September 30, 1999, the appellant physician had a 14% infection rate from one procedure and a 7.9% overall infection rate. This was quadruple the national rate for physicians in his specialty. After a further peer review of the appellant's charts by an outsider review, the physician's staff privileges were limited. The Midas program played a useful preliminary role in identifying files that fell outside the parameters of the program, generating a statistical flag that triggered peer review of the appellant's charges.

A second case is *Lo v. Provena Covenant Medical Center.*[81] A review of patient statistics from the hospital's cardiovascular-surgery program revealed that Dr. Lo, one of two cardiovascular surgeons on the medical staff, had a high rate of mortality compared to national norms (5.3% compared to 3%) and a high complication and readmission rate. For the two cardiovascular surgeons on the hospital's staff, the mortality rate was 7%, the rate of return to surgery after surgery was 13.1% and the rate of hospital readmission within thirty days was 19.3%. The mortality rate for plaintiff's patients was 5.3% in 2000, 5% in 2001 and 5% in 2002. By contrast, during the same period, the national rate of mortality for open-heart surgery was 3% in 2000 and 2.3% in 2001. "The hospital itself has inherent authority to summarily suspend clinical privileges to prevent an imminent danger to patients. To that end, the chief executive officer can impose a summary suspension on the authority of the hospital board."[82] The president of the medical center, faced with apparent unwillingness by the medical staff to get involved in the various limitations imposed on Dr. Lo, met with the executive committee of the board of directors. The Committee authorized President Friedman to suspend summarily plaintiff's clinical privilege to perform open-heart surgery. The court held that if danger to patients is genuine and imminent, the hospital governing board has a duty to protect patients by summarily suspending the privilege of a physician when data shows that a mortality rate is well above the norm.[83]

[79] 113 Cal. Rptr. 2d 309 (Cal. Ct. App. 2001).

[80] ACS's Midas+ Comparative Performance Measurement System is a performance improvement software application that provides comparative data to over 250 hospitals nationally, with large databases housing over fourteen million encounters. *See* Affiliated Computer Services, *supra* note 70 (describing software).

[81] 796 N.E.2d 607 (Ill. App. Ct. 2003).

[82] *Id.* at 615 (internal citation omitted).

[83] *See id.* at 614 (finding that "hospital has inherent right to summarily suspend the clinical privileges of a physician whose continued practice poses immediate danger to patients").

Discovered data about performance may help a conscientious provider. For example, in *Nugent v. Saint Agnes Medical Center*,[84] the hospital's peer review committee conducted a ten-day evidentiary hearing and found that Doctor 257's treatment of ten hospital patients showed deficiencies. His infection rate for all orthopedic surgeries from January 1, 1999 to September 30, 1999 was 7.8% and for lumbar laminectomy/fusion procedures, it was 14%. No other physicians, including all other orthopedists at St. Agnes, exceeded 4%. The information was surprising to the physician. He implemented changes in his hospital practices, and the infection rate for his patients dropped to zero, despite a statistically meaningful number of surgeries, and the rate remained zero up to the time of trial.

What is the source of bad outcomes? It is often hard to identify. It might be depression, substance abuse, lack of skill, poor team support in the surgical suite, a flaw in the hospital pharmacy, a flaw in the hospital's management or scheduling or records systems. The use of computer generated statistical profiles of provider performance and patient outcomes will likely move health care toward a difficult and defensive environment, at least in the near term, as providers struggle to disentangle themselves from a data web that shows them to be outliers—poor performers. Staff privilege cases show the power of computer programs like Midas in detecting poor quality care. Such profiling and comparative data use may be protective of both providers with painful secrets and patients with confidential conditions that they want kept private. In a new health care economy where all that matters is performance—measured by positive patient outcomes—we may have less motivation to tinker with the legal system to force disclosure of provider secrets or to dig into patient confidential data to explain bad performance.

2. *Corporate Negligence*

A patient injured in the hospital may argue that the hospital was negligent in retaining a physician on the medical staff, if outcome data compiled by the hospital reveals that the physician was at the very bottom of the staff profile. The corporate negligence doctrine, accepted in many American states, defines a hospital's duties in four different areas: (1) reasonable care in maintaining safe and adequate facilities and equipment; (2) selection and retention of competent physicians; (3) oversight of all those who practice medicine within the hospital's walls; and (4) creation, adoption and enforcement of policies adequate to ensure quality care for patients.[85]

Imagine a hospital with detailed risk information on all of its physicians, surgical teams and so on. If that hospital fails to act to limit staff privileges, to shift staff around and to improve support in deficient areas, a

[84] No. F043928, 2004 WL 2953326 (Cal. Ct. App. Dec. 21, 2004).

[85] *See, e.g.*, Thompson v. Nason Hosp., 591 A.2d 703, 707 (Pa. 1991) (listing elements of corporate negligence doctrine).

plaintiff could successfully argue corporate negligence. Current tort law requires a health care provider to gather such information carefully, as the standard of care evolves toward systematic data collection of outcomes, and to monitor regularly the outcomes of individual physicians. A properly designed outcome measurement system, using data mining techniques, will produce data as to unnecessary procedures, high error rates and other early warnings of problems with a staff physician.[86] The existence of such a process will give a hospital actual notice of a problem, leading to liability.[87] A hospital is under a duty to restrict the clinical privileges of staff physicians who are incompetent to handle certain procedures, and to detect concealment by a staff doctor of medical errors. While some courts have limited this duty to only those situations where a hospital has learned of physician insufficiencies,[88] others have talked of "negligent supervision" in terms of an affirmative duty to detect problems.[89]

Data mining is likely to produce firm statistical distributions that will allow the generation of inferences, akin to those of *res ipsa loquitur*, that a patient injury is more properly attributable to provider negligence than innocent explanations, recognizing the increased statistical likelihood that a provider is to blame in the particular case. Whether a court would be willing to use such data in a negligence case as the basis for a *res ipsa*

[86] Critics point out a variety of problems with requiring disclosure of such data at present. First, because data is never perfect—given different patient conditions—use of data may shift patients away from a poorer provider or affect its reimbursement. This will lead to gaming the system, if possible, as providers scramble to adversely select against poorer cases in order to improve their track record. Second, quality differences may not always be fixable. Some doctors will be better and some organizations are better managed. Self-improvement based on data will fall short where poor management cannot recognize bad processes. Third, we will always have to make tradeoffs between more or less effective care and its cost. The tradeoff between uncertainty and cost will always remain. Fourth, some relatively good providers will suffer because of invidious performance comparisons, given imperfect data and patient variation. Some good providers will therefore be lumped with the larger pool of incompetent or less competent providers. For criticisms of medical performance statistics and cautions that provider-specific outcome statistics must be carefully evaluated to insure their reliability and validity when used as evidence, see, for example, Jesse Green, *Problems in the Use of Outcome Statistics to Compare Health Care Providers*, 58 BROOK. L. REV. 55 (1992); Rheingold, *supra* note 54.

[87] *See* Cronic v. Doud, 523 N.E.2d 176, 178-79 (Ill. App. Ct. 1988) (showing case where unnecessary surgery by physician should have been detected by hospital through utilization review, because it had data to put it on notice of problem). *Contra* Reynolds v. Mennonite Hosp., 522 N.E.2d 827, 829-30 (Ill. App. Ct. 1988), *reh'g denied*, 530 N.E.2d 264 (Ill. 1988) (granting summary judgment for hospital on same facts as *Cronic v. Doud*, but plaintiff had not pleaded utilization review data).

[88] *See* Albain v. Flower Hosp., 553 N.E.2d 1038, 1046 (Ohio 1990) ("Nor is a hospital required to constantly supervise and second-guess the activities of its physicians, beyond the duty to remove a known incompetent.").

[89] *See, e.g.*, Oehler v. Humana, Inc., 775 P.2d 1271, 1272 (Nev. 1989) (discussing what is necessary to prove negligent supervision).

instruction is another question, but certainly one worth arguing if the data is made available and peer review privilege or other statutory immunities are not available as a defense.

Another possible consequence of systematic data mining is that variable provider performance will be discovered, as the staff privilege cases above have indicated. This may lead to a recommendation that physician performance be tested and reevaluated regularly. One author, Sissela Bok, has argued that we should treat doctors as seriously as we treat pilots, recognizing the lives they can affect if they are slipping in competence or have other problems in their lives.[90]

Current tort law requires a health care provider to gather such information carefully, as the standard of care evolves toward systematic data collection of outcomes, and to monitor regularly the outcomes of individual physicians. A properly designed utilization review process within an institution will produce data as to unnecessary procedures, high error rates and other early warnings of problems with a staff physician. The existence of such a process will give a hospital actual notice of a problem, leading to liability. A hospital is also under a duty to restrict the clinical privileges of staff physicians who are incompetent to handle certain procedures and to detect concealment by a staff doctor of medical errors.[91]

B. *Patient Safety and Quality Improvement Act—Is Concealment the Likely Result?*

Modest JCAHO and Center for Medicare and Medicaid Services (CMS) reporting requirements and audits strive to create a state of "forced mindfulness" by providers, as the data forces feedback as to sources of bad outcomes and the resulting ability to fix problems.[92] The proliferation of state error reporting legislation clearly is designed to push hospitals to track adverse events and near misses resulting from hospital treatment and report to the state, and often to the patient. The federal effort until recently, however, has been quite modest. The 2005 Patient Safety and Quality Improvement Act (the "Act") is one of several new federal initiatives to promote data generation and disclosure within hospitals. The Act authorizes the creation of "patient safety organizations" that will conduct

[90] One commentator notes:

> For while alcoholism and related conditions afflict persons in every walk of life, they cause the disabled physician to be especially dangerous. People can deteriorate in many kinds of work; but the effects, while serious in the long run, will rarely be as catastrophic for innocent victims as when a false diagnosis is made, the wrong medication prescribed, or incompetent surgery performed.

SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 165 (1978).

[91] *See* Lo v. Provena Covenant Med. Ctr., 796 N.E.2d 607, 614 (Ill. App. Ct. 2003) (finding that "hospital has an inherent right to summarily suspend the clinical privileges of a physician whose continued practice poses an immediate danger to patients").

[92] *See generally* Furrow, *supra* note 33.

"patient safety activities" within hospitals and other health care institutions.[93] Such patient safety work product is any data, reports, records, memoranda, analysis or written or oral statements "which could result in improved patient safety, health care quality, or health care outcomes."[94] The heart of this new legislation is the federal certification of patient safety organizations (PSOs), governed by the Agency for Healthcare Research and Quality, which is good for three years. These PSOs would collect reports of medical errors voluntarily submitted by health care providers for inclusion in a patient safety network of databases. Results would be analyzed and disseminated to providers including recommendations, protocols or other guidelines describing best practices.

The Act creates a federal privilege for patient safety work product, preempting states' laws governing civil or administrative procedures that require the disclosure of information by a health care provider to a certified PSO. Providers could report voluntarily and confidentially all errors through a "Patient Safety Work Product (PSWP)" to a certified PSO. Such work products are not subject to discovery, disclosure under the Freedom of Information Act, admissibility in any Federal, state or local government proceeding or disciplinary proceeding under state law. They are also confidential and may not be disclosed. Exceptions to confidentiality include disclosure to carry out patient safety activities, non-identifiable patient safety work product, to grantees for research, demonstration projects and so on. JCAHO is specifically considered, as the Act expressly allows "[v]oluntary disclosure of patient safety work product by a provider to an accrediting body that accredits the provider."[95] The Act also provides that:

> A patient safety organization shall not be compelled to disclose information collected or developed under this part whether or not such information is patient safety work product unless such information is identified, is not patient safety work product, and is not reasonably available from another source.[96]

Further, the Act specifies that:

> An accrediting body shall not take an accrediting action against a provider based on the good faith participation of the provider in the collection, development, reporting, or maintenance of patient safety work product in accordance with this part. An accrediting body may not require a provider to reveal its

[93] *See* Patient Safety and Quality Improvement Act of 2005, Pub. L. No. 109-41, § 924, 119 Stat. 424, 431-34 (2005) (describing process for entities to become patient safety organizations).

[94] *Id.* § 921(7)(A)(i)(II), 119 Stat. 426.

[95] *Id.* § 922(c)(2)(E), 119 Stat. 428.

[96] *Id.* § 922(d)(4)(A)(i), 119 Stat. 428-29.

> communication with any patient safety organization established in accordance with this part.[97]

The new Act provides no mandate for systematic data collection by providers, nor any reimbursement for it. It does not compel use of data in any kind of national reporting system. Moreover, it fails to make a serious and systematic attempt to tie performance to solid measurements and to reimbursement.[98] Hospitals or their medical staffs are likely to want to take advantage of the immunities provided, however, and will establish their own PSOs for their own confidential and privileged safety program. This is bound to have a positive effect on data gathering and performance measurements.[99] This new legislation may even have the effect of accelerating the use of data mining and its consequences within institutions, even though its primary thrust is the creation of a federal privilege for patient safety work products.

V. CONCLUSION

Physicians should welcome mining of aggregate data. The focus will shift from their habits, proclivities and politics, to their performance. Therefore, the HIV-positive physician, the older doctor and the substance abuser, will be measured more by the measurable risks they create, and less by their status. There will be surprises, but also repairable situations for some physicians. Ultimately, patient care is bound to benefit. Hospitals may have no choice but to welcome data mining, whether they like it or not. The inexorable pressures of HIPAA, of Medicare reimbursement pressures and state adverse event disclosure laws, all suggest that data mining is a useful tool along with systematic error and near miss disclosure requirements, for detecting patterns of patient harm. Hospitals should aspire to zero defects, just as the best industries do.

[97] *Id.* § 922 (d) (4) (B), 119 Stat. 429.

[98] *See* AM. MED. ASS'N, SUMMARY OF S. 544, http://www.ama-assn.org/ama/pub/category/15341.html (last visited Apr. 22, 2006) (providing synopsis of major provisions of Patient Safety and Quality Improvement Act of 2005).

[99] *See* PATIENT SAFETY NETWORK, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, http://psnet.ahrq.gov (last visited Apr. 22, 2006) (providing new national web-based resource featuring latest news and resources on patient safety, including weekly updates of patient safety literature, news, tools and meetings).