OPPORTUNITY LOST: WHY AND HOW TO IMPROVE THE HHS-PROPOSED LEGISLATION GOVERNING LAW ENFORCEMENT ACCESS TO MEDICAL RECORDS

PETER H.W. VAN DER GOES, JR.†

INTRODUCTION

Imagine a "not-too-distant" time when "genetic screening is the norm and the upper strata of society are closed to people who haven't been created through science. In-Valids, they're called . . . ."[1] Genetic science has progressed to the point where every human trait can be engineered, and society now stigmatizes, discriminates against, and even pities those unfortunate enough to be conceived the old-fashioned way. In this world, those who are the product of "faith birth[s]" must lie and deceive to gain access to those areas they desire.[2] Thus, for an "In-Valid" to pursue the dream of becoming, say, an astronaut, "he must be genetically perfect, and since true identity can be established instantly by examination of just one cell, any cell, from his body, the deception involved in becoming the person he wants to be is fascinatingly elaborate and difficult."[3]

As a chilling corollary, the institutions and organizations that regulate and order our society—corporations, governments, and law enforcement agencies—have access to the information contained in individuals' genes

---

† B.A. and B.S. 1991, University of Pennsylvania; M.B.A. 1998, University of Pennsylvania; J.D. Candidate 1999, University of Pennsylvania. Many student authors have expressed heartfelt appreciation for the efforts of the *University of Pennsylvania Law Review* editors. To such acknowledgements I would add an apology—my own shortcomings in ability and effort not only have resulted in any remaining errors, but also undoubtedly have left many an editor with more work than was wanted, or deserved. I would also like to thank my parents James and Camille, whose guidance and support through school have been indispensable. I am most grateful, however, to my wife Jody. She has made this, and all else, possible.

[1] Shawn Levy, "Gattaca," PORTLAND OREGONIAN, Dec. 26, 1997, at 19, *available in* 1997 WL 13148446 (reviewing GATTACA (Columbia Tri-Star 1997)).

[2] Brian McTavish, "Gattaca" *Has Science and Fiction and Soul*, KAN. CITY STAR, Oct. 24, 1997, at 14, *available in* 1997 WL 3028557 (discussing the need for deception by In-Valids in order to rise above certain social strata in the movie *Gattaca*).

[3] Rene Downing, "Gattaca" *Premise: Future's Not in Stars, but in Our Genes*, ARIZ. DAILY STAR, Nov. 20, 1997, at 1C, *available in* 1997 WL 7934923 (reviewing GATTACA (Columbia Tri-Star 1997)).

via their medical histories and records. In this vision of the future, corresponding technological advances in information storage, retrieval, and access have accompanied the advances in genetic technology. Thus, the forensic capabilities of the police to investigate crimes such as murder, and the totality of their access to the private medical and genetic records of citizens, reminds one of the bleak and grotesque futures envisioned by Huxley and Orwell.[4]

Of course, many people would recognize the world just described as a fantasy, created by writer/director Andrew Niccol in his 1997 science-fiction thriller *Gattaca*.[5] Similarly, few Americans would take seriously the notion that government authorities collect genetic samples from almost all of us, keeping and cataloging these samples indefinitely. This, however, is a reality: hospitals take blood samples from virtually every newborn in the United States and store a bloodspot on a card.[6] These samples, known as "Guthrie spots,"[7] remain stable for many years and can reveal genetic data indefinitely when properly preserved. In 1994, three-quarters of the states stored Guthrie-spot cards, and at least four intended to do so indefinitely.[8] Combine this with the push to create a single national health information database using individual identifiers,[9] and the world Niccol envisions in

---

[4] *See* ALDOUS HUXLEY, BRAVE NEW WORLD (1932) (portraying a fictional future in which the government pervades and controls individuals' lives); GEORGE ORWELL, 1984 (1949) (describing a fictional world where "Big Brother" and the "Thought Police" represent extreme forms of governmental intrusion and control).

[5] *See* GATTACA (Columbia Tri-Star 1997) (presenting a world in which genetic engineering is both feasible and necessary to achieve social status, and depicting a genetically imperfect person's struggle to achieve his life's goal of space travel in the face of legal and social barriers); *see also* Bob Kurson, *Dabbling in DNA: "Gattaca" Director Exploring Ethics*, CHI. SUN-TIMES, Nov. 16, 1997, at 7-NC, *available in* 1997 WL 6379554 (discussing the premise and issues explored in the film).

[6] *See* Jean E. McEwen & Philip R. Reilly, *Stored Guthrie Cards as DNA "Banks,"* 55 AM. J. HUM. GENETICS 196, 196-97 (1994) (describing the possibility of using dried blood spots on Guthrie cards as a source of DNA for research or testing purposes).

[7] Guthrie Spots are named for their inventor, Dr. Robert Guthrie. *See* Robert S. Boyd, *Nation's DNA Databanks Threaten Privacy*, ATLANTA J. & CONST., Nov. 6, 1994, at H1.

[8] *See* McEwen & Reilly, *supra* note 6, at 196-97 (noting that 37 of the 50 states, plus the District of Columbia, Puerto Rico, and the Virgin Islands "retain all the Guthrie cards that they receive through their newborn-screening programs" and that four states keep their cards indefinitely, with several other states considering "a permanent-retention policy"); *see also* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 468 (1995) (noting that other "tissue repositories" have been created and maintained especially for genetic research). In 1994, four states had "saved more than a million cards apiece, and California alone ha[d] more than six million" stored cards. Boyd, *supra* note 7, at H1.

[9] *See, e.g.*, Arthur Allen, *Exposed*, WASH. POST, Feb. 8, 1998 (Magazine), at 13 ("The Clinton administration's aim is to help create a seamless nationwide records system that eventually may involve a 'universal patient identifier,' the equivalent of a Social Security number for each patient.").

Gattaca may be a fantasy only with respect to the genetic engineering. Indeed, the level of governmental information access and control Niccol describes is well within our government's vision and grasp.

Not surprisingly, Americans expect and assume that medical records privacy is a primary and well-defended right in our society. For example, numerous studies confirm that we consider medical records privacy extremely important,[10] that we expect vigilance with respect to medical professionals protecting this privacy,[11] and that we are concerned that changes in information technology threaten this privacy.[12] Undoubtedly, the rapid and fundamental changes in technology, information systems, and the health care industry have created an environment in which medical records are more accessible, and more frequently accessed, than anyone imagined even

---

Under the Health Insurance Portability and Accountability Act ("HIPAA" or "the Act"), the Department of Health and Human Services ("HHS") is required to create a unique identification number for every person, provider, health plan, and employer. *See* 42 U.S.C. § 1320d-2(a) to (b) (Supp. II 1996) (establishing both the standards for enabling the electronic exchange of health information and the need to adopt standards for the creation of a unique health identifier). Last summer, however, as the Clinton administration pulled back from its push for a framework for such a system, it became apparent that such a system of unique patient identifiers would not be put into use until confidentiality legislation was passed in accordance with HIPAA's provisions. *See* Frank James, *ID-Number Proposals Raise Issue of Privacy*, CHI. TRIB., Aug. 31, 1998, § 1, at 6 ("Vice President Al Gore announced the delay [of HHS's development of the unique patient identifier system] last month during a speech in which he detailed administration initiatives meant to address Americans' worries about privacy."). Given the tremendous economic benefits that would result from such a system for many constituencies in the health care industry, however, it seems likely that this is a delay in its development, not an end to the initiative. *See, e.g.*, Sheryl Gay Stolberg, *Health Identifier for All Americans Runs into Hurdles*, N.Y. TIMES, July 20, 1998, at A1 ("Proponents, including insurance companies and public health researchers, say the benefits would be vast."). Indeed, despite Gore's announcement, the government remains actively engaged in promoting a standard system. *See, e.g.*, Judy Foreman, *Your Health History—Up for Grabs?*, BOSTON GLOBE, July 20, 1998, at C1 ("In October [1997], the Sequoia Software Corporation in Columbia, Md., won a multi-million dollar grant from the US Commerce Department to develop a national 'Master Patient Index.' The goal, the company said, is to develop a 'massively distributed medical records system across a national computer backbone.'").

[10] A 1996 CNN/*Time* poll indicates that 87% of Americans want to be asked permission every time their medical records are accessed for any reason. *See* Alissa J. Rubin, *Gore to Propose More Privacy Safeguards for Public*, L.A. TIMES, July 31, 1998, at A26 (citing the results of the CNN/*Time* poll).

[11] *See* JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE 51 (2d ed. 1991) (reporting the results of a 1990 poll indicating that the respondents assumed that hospitals would afford them a high degree of confidentiality relative to other professionals and entities in society).

[12] *See* ALAN F. WESTIN ET AL., LOUIS HARRIS & ASSOCS., HEALTH CARE INFORMATION PRIVACY: A SURVEY OF THE PUBLIC AND LEADERS 66-67 (1993) (indicating that 64% of the public is concerned that computers create an opportunity for unauthorized access to private medical information).

ten years ago.[13] Because of this evolution, a broad coalition of privacy advocates, citizens' groups, and legal scholars have called for the federal government to replace the inconsistent and incomplete patchwork of state and federal laws protecting the medical records privacy rights of citizens with a single, strong federal law.[14]

The efforts of that coalition came to fruition in the fall of 1997, when, in response to HIPAA, passed on August 21, 1996,[15] HHS issued a report laying out its recommendations for a federal law.[16] Despite some special-interest criticisms,[17] many felt that the report, entitled *Confidentiality of Individually-Identifiable Health Information* ("*HHS Report*" or "the *Report*"),[18] reflected a legitimate interpretation and representation of the best aspects of constitutional and judicial protections of medical records privacy in the computer age.[19] There was one area, however, where HHS appeared to shrink from its strong position of privacy protections: the general exception for law enforcement access to medical records[20] was left unmodified

---

[13] Numerous commentators have described this combination of developments. *See, e.g.*, Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 300-06 (1995) (describing the increasing role of data processing in health care). For a brief exploration of these changes, see *infra* Part II.A.

[14] *See* Allen, *supra* note 9, at 15 (explaining how congressional reform proposals have been "based on months of consultation with privacy experts, industry and Congress" in order to obtain "some kind of confidentiality law").

[15] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.).

[16] The issuance of this report was highly anticipated and widely covered, with dozens of newspapers and special-interest information sources reporting it. *See, e.g.*, *Insurers Fear a Strict Federal Privacy Law*, INS. REGULATOR, Sept. 22, 1997, at 1, *available in* LEXIS, News Library, CURNWS File (representing an example of the special-interest coverage of the report's issuance).

[17] *See, e.g.*, *id.* at 1 (noting that representatives of the workers' compensation and auto insurance industries warned that the HHS proposals might interfere with claims evaluation); *Medical Records: HHS Proposes Privacy Standards*, HEALTHLINE, Sept. 12, 1997, at 3 ("Herbert Sacks, president of the American Psychiatric Association, disagreed with the proposals.").

[18] DEPARTMENT OF HEALTH AND HUMAN SERVICES, CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION: RECOMMENDATIONS OF THE SECRETARY OF HEALTH AND HUMAN SERVICES, PURSUANT TO SECTION 264 OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (last modified Sept. 10, 1997) <http://www.epic.org/privacy/medical/hhs_recommendations_1997.html> [hereinafter HHS REPORT].

[19] *See, e.g.*, *HHS Privacy Plan Due this Week*, WASH. HEALTH WK., Sept. 8, 1997, at 2, *available in* 1997 WL 9048137 (noting general approval for the *HHS Report*'s contents by the American Health Information Management Association, representing a broad cross section of the health care industry).

[20] To describe this exception to the general rule of medical records privacy, I frequently use the term "law enforcement exception." This term is meant to encompass the related set of legal principles that allow law enforcement (for example, inter alia, local, municipality, and

and unregulated,[21] despite compelling reasons for imposition of federal guidelines in this sphere.[22]

This Comment argues for increased federal protections against law enforcement intrusion into personal medical records under the set of law enforcement exceptions to the general legal principles establishing medical records privacy. Although it is important to recognize that law enforcement authorities, like other information users, often have legitimate reasons for accessing such personal information, there are strong legal and societal rationales for drafting clear federal-level protections against unwarranted intrusions by law enforcement personnel. Profound changes in medical and information technology have driven our reevaluation of privacy protections with regard to other non-law-enforcement users of personal medical information.[23] Similarly, we should reexamine law enforcement access to such information in light of these dramatic changes.

A critical examination of the proposed law enforcement exception first requires an understanding of the technological and legal context of the *HHS Report*. As a result, Part I of this Comment outlines the changes in medicine and medical record keeping that gave rise to HIPAA and the *HHS Report*. This Part contains a brief overview of the Act and resulting *Report*. It also discusses the manner in which these proposed rules recognize the changing realities of medical and information technology, and contrasts the general thrust of the *Report* with the policy behind the proposed law enforcement exception.

Part II then reviews the legal foundations for the current law enforcement exception standard. This Part demonstrates that legal principles exist that support strong limitations on law enforcement's access to personal medical records. Part II also surveys the impediments to such limitations reflected in the constitutional context, federal statutory framework, and state-level legal structures. The shortcomings and inconsistencies of this patchwork of legal protections against unwarranted access to medical rec-

---

state police; federal law enforcement officers; federal agencies charged by statute with enforcement of the laws under which they operate) to obtain access to what would otherwise be considered private individual medical records, protected by the legal standards discussed in Part II of this Comment.

[21] *See infra* text accompanying note 98 (quoting the *HHS Report*'s recommendation to leave unchanged the current broad access of law enforcement to medical records).

[22] *See infra* Part III (criticizing the *HHS Report*'s failure to address the need for a federal law governing law enforcement's use of private medical records in its proposed law enforcement exception).

[23] *See, e.g.*, Schwartz, *supra* note 13, at 300-09 (describing the increased use of information technology and information collection in health care records and proposing changes in privacy protections).

ords by law enforcement personnel, it is argued, cuts in favor of establishing stronger, more uniform limitations at the federal level.

Part III explores this federal uniformity argument and others. In general, Part III develops the major legal and policy arguments for revisiting the *HHS Report*'s position on law enforcement access to medical records. These arguments incorporate a review of the moral and social benefits achieved in creating a clear federal standard. They also recognize a host of related issues, including the demands of technological change, the need for greater protection of acknowledged constitutional rights, and the need to re-evaluate other legal frameworks. Additionally, this Part considers the potential problems in administering the *Report*'s proposed penalties-based approach.

Part IV offers some suggestions on how the proposed law enforcement exception could be modified to address the arguments discussed in Part III while still accommodating law enforcement information needs. This Part recognizes and evaluates commentators' suggestions for strengthening HHS's proposed law, and develops a general and straightforward set of recommendations that, if adopted, would create a legal framework that embraces a more vigorous set of privacy protections without undue harm to law enforcement's ability to achieve its aims. This framework acknowledges the limitations of individuals' privacy rights with respect to their medical records. In the face of these limits, however, it offers substantially sufficient protections in the increasingly complex world of medical and information technology, and law enforcement's increasingly invasive use of this information.

I. TECHNOLOGICAL AND SOCIETAL CHANGES DRIVING HIPAA AND THE *HHS REPORT*

When Congress included medical records privacy language in HIPAA, it was not only recognizing the sweeping changes that took place in medical records information management and utilization, but was also attempting to address the impact that future industry changes would have on individuals' privacy. This Part provides a limited introduction to the nature and scope of the changes in health care information technology and records management and how these changes have been driven by larger influences in health care delivery. It also introduces the legislation at issue, HIPAA, and the resulting *HHS Report*, discussing the structure and principles that seem to guide the *Report*'s legislative suggestions, while focusing in particular on the law enforcement exception.

A. *The Health Care Industry, Technology, and the Falling Away of Medical Records Privacy*

Three factors have driven the evolution in the use of medical records and health information technology: (1) changes in information technology; (2) increasing demands for medical research and the need for research data; and (3) the for-profit shift in health care delivery.[24] These changes have driven unforeseen shifts in the collection, use, and dissemination of personal data through the health care system.[25] The extent and fundamental nature of these changes is difficult to overemphasize.

1. The Rise of Information Technology and Its Effect on Medical Records Privacy

As noted above, the American public is concerned about the potential loss of privacy that could result from the increasingly complex and ambitious scope of medical record information systems.[26] When looking at the changes in how the health care industry uses technology to collect, manage, and access data, it appears that the public is justified in its concern. In 1995, Lawrence Gostin, a noted medical ethicist and legal scholar, observed that "[p]lans for the systematic collection, storage, use, and dissemination of a huge volume of uniform data sets in electronic form [were] already under way and [had] an aura of inevitability."[27] Three years later, a number of sources confirmed Gostin's assertion that information technology would transform the use and distribution of medical records in a fundamental way.[28] Specifically, they observed that these very advances in electronic

---

[24] *See, e.g.*, Schwartz, *supra* note 13, at 300-06 (discussing the changes in health care and medical records uses); Allen, *supra* note 9, at 11-15 (reviewing some of these factors in the changes in health care).

[25] *See, e.g.*, Doug Stanley & Craig S. Palosky, *Electronic Storage Opens New Chances for Abuse*, TAMPA TRIB., Feb. 17, 1997, at 1, *available in* 1997 WL 7035400 [hereinafter Stanley & Palosky, *Electronic Storage*] (arguing that changes in information technology can improve health care, but also threaten privacy because of information dissemination); Doug Stanley & Craig S. Palosky, *Privacy Lost*, TAMPA TRIB., Feb. 16, 1997, at 1, *available in* 1997 WL 7035275 [hereinafter Stanley & Palosky, *Privacy Lost*] (describing an employer's use of an employee's private medical records in *Doe v. Southeastern Pennsylvania Transit Authority*, 72 F.3d 1133 (3d Cir. 1995)).

[26] *See supra* note 12 and accompanying text (indicating that over 60% of the public believed that computer systems created unauthorized access problems in the area of confidential medical records).

[27] Gostin, *supra* note 8, at 452.

[28] There is ample statistical and anecdotal evidence of this revolution. For example, Arthur Allen notes that:

> Health care providers are currently spending around $2 billion a year to build new information networks that support approaches such as "disease management," which

information systems create the opportunities for improper access.[29] In March 1997, the National Research Council[30] released a report decrying the lack of security of electronic medical records and warning that the increasing use of computer systems to gather, hold, and manipulate personal health information was creating a serious threat to privacy rights of patients.[31] Undoubtedly, changes in information systems technology could create a need for new legal protections of privacy that work within the shifting context wrought by these changes.[32]

2. The Escalating Needs of Medical Researchers

Also driving the need for improvements in privacy protections for medical data are the changes in medical research and research data collection. Innovations in information systems technology have improved researchers' ability to collect, store, and interpret increasingly larger sets of

---

> consists in part of computerized programs that help prod sick people into getting particular kinds of treatment. At Harvard Pilgrim Health Care in Boston, for example, information specialists scanned the company database and located all patients who had had expensive emergency room visits more than three times. Many of them, it turned out, were alcoholics. Thereafter, when one of the patients entered an emergency room, his or her primary physician was notified and instructed to talk to the patient.

Allen, *supra* note 9, at 15; *see* Craig S. Palosky & Doug Stanley, *Computer Full of Secrets*, TAMPA TRIB., Feb. 18, 1997, at 1, *available in* 1997 WL 7035604 (reporting on Florida health officials' development of a statewide information database that began requiring Social Security numbers in 1995); Stanley & Palosky, *Privacy Lost*, *supra* note 25, at 1 (describing the employer's health care information collection and use at issue in *Doe*, 72 F.3d at 1135-37).

[29] *See* Jean Hellwege, *Security Problems Plague Financial, Medical Record Keepers*, TRIAL, June 1997, at 22 ("[T]he online storage and transmission of these records have made it easier for computer-savvy snoops to access them.").

[30] The National Research Council is "a part of the National Academy of Sciences, a private organization chartered by Congress to conduct research at the request of government agencies." Paul Recer, *Radon Linked to 21,800 Deaths*, CHATTANOOGA TIMES, Feb. 20, 1998, at E12, *available in* LEXIS, News Library, Papers File.

[31] *See* NATIONAL RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 3 (1997) ("Within individual organizations, electronic information systems and [electronic medical records] are potentially vulnerable to misuse from both authorized users and unauthorized outsiders who inappropriately access patient information for their personal or economic gain.").

[32] *See, e.g.*, Françoise Gilbert, *Privacy of Medical Records? The Health Insurance Portability and Accountability Act of 1996 Creates a Framework for the Establishment of Security Standards and the Protection of Individually Identifiable Health Information*, 73 N.D. L. REV. 93, 93-95 (1997) (discussing technological changes in medicine and the resulting need for federal legislation); Gostin, *supra* note 8, at 516-17 (advocating that changes in technology mandate the need for federal laws in this area); Schwartz, *supra* note 13, at 300-38 (arguing that changes in data collection and usage require a reevaluation of general privacy law); Allen, *supra* note 9, at 13-14 (observing generally the trend toward legislative changes that have resulted or will result from these technology advances in medical records management and use).

data. For example, the National Health and Nutrition Examination Survey exemplifies a relatively recent effort to create a comprehensive medical research database.[33] This database contains broad health status data in patient-identifiable[34] form on 40,000 individuals.[35] The subjects are examined, and hundreds of data elements are collected from each person.[36] There is no doubt that such ambitious accumulations of medical data would not be possible without modern database technology, in large part because access to such data is made easier by the electronic format in which it is stored. Commentators have recognized the growing relationship between the increasing research interest in health information databases and the increasing computerization of such information. William Lowrance, in his report to HHS on research and privacy, noted that "[a]s databases are maturing and increasing in size and quality, their appeal as research resources also is growing. Thus the databases of healthcare finance systems and managed-care organizations, among others, are much in demand. These large collections of standardized, computerized data have much information to yield."[37] Certainly, the evolution of private health information management has

---

[33] *See* NATIONAL CTR. FOR HEALTH STATISTICS, U.S. DEP'T OF HEALTH AND HUMAN SERVS., PLAN AND OPERATION OF THE THIRD NATIONAL HEALTH AND NUTRITION EXAMINATION SURVEY, 1988-1994, at vi (1994) [hereinafter NATIONAL CTR. FOR HEALTH STATISTICS] (describing the survey as a "mammoth national study").

[34] "Patient-identifiable" is a term of art used in the health care information technology industry to describe medical record data that can be used to trace the information back to an identifiable, individual patient. Interview with Mark Davidson, Health Care Information Technology Consultant, First Consulting Group, Inc., in Phila., Pa. (Oct. 4, 1997).

[35] *See* NATIONAL CTR. FOR HEALTH STATISTICS, *supra* note 33, at 1 (noting that the goals of the survey "included the need for precise descriptive information on the health status of selected population groups of the United States and required that these groups be sampled in large proportions to ensure the precision of the information").

[36] *See id.* at 48-62 (listing the dozens of blood and urinary data assessments, almost 100 assays and related analyses, the 20 general exam types, the areas of nutrition-related data collected, other findings reported, and the over 100 lab tests reporting categories used during the study).

[37] WILLIAM W. LOWRANCE, PRIVACY AND HEALTH RESEARCH: A REPORT TO THE U.S. SECRETARY OF HEALTH AND HUMAN SERVICES 62 (1997). Also, much research is done on data collected for other non-research purposes. For instance, extensive research efforts are based on data collected by the Health Care Financing Administration's Medicare and Medicaid databases; these repositories contain perhaps the largest collection of health data in the world. *See id.* at 18-19 ("Perhaps the largest collection of health databases in the world is the . . . U.S. 'Medicare' database systems . . . ."). Note that such research efforts do not necessarily contribute to the growth of health information's electronic collection and storage. Yet such secondary uses certainly multiply the number of users of private health information, and research demands can often affect governmental collection and treatment of private health-related data even when the primary goal of collection is to further non-research aims. *See id.* at 19 (noting that the Health Care Financing Administration creates "[p]ublic-use" files of confidential medical data for research purposes when the data in its original form was for "administrative and billing" records).

driven the desire for researchers to collect data and use existing private data collections in previously unintended ways.

3. Health Care Industry Changes

The most important factor driving the need for changes in medical record privacy laws is the fundamental change in the delivery and financing of health care. These changes are characterized by an increasing demand by payors (employers, individuals, and the government) to drive costs downward, and the resulting shift to a for-profit focus in medical service provision, as formerly non-profit institutions are replaced by publicly-traded companies.[38] These economic forces have resulted in a dramatic shift in how health care is delivered to insured patients. Nine years ago, fewer than twenty-five percent of insured Americans received health care in a managed-care environment; as of 1998, over eighty-five percent of those insured in this country obtain care through a service delivery system that contains at least "significant" forms of cost management.[39]

This transformation results in services where costs are sharply in focus, and those providing services seek to reduce costs in increasingly sophisticated ways.[40] One consequence of this is that providers use information systems not only to collect and manage insurance payments and to verify service provisions, but also to help change medical practice in an effort to reduce costs or improve profits.[41] Hospitals, nursing homes, and physician

---

[38] Interview with Howard Capek, Medical Services Research Analyst, Credit Suisse First Boston, in N.Y., N.Y. (Dec. 19, 1997) (discussing generally the increasing profit motive in health care services provision, and the rise of for-profit hospital chains in particular).

[39] Linda Burns, Vice President, Columbia/HCA Inc., Health Care Finance Class Lecture at the Wharton School, University of Pennsylvania, in Phila., Pa. (Mar. 23, 1998) (lecturing on the transformation of the health care services industry that resulted from this change in payor mix).

[40] Interview with Howard Capek, *supra* note 38 (discussing utilization review, cost management via preventative care, and other information technology efforts undertaken by health care providers in an effort to reduce costs through improved information management and analysis).

[41] *See id.* (discussing Genesis/Eldercare, a long-term care company, and its implementation of information systems to track pertinent data in an effort to create standardization of care that will drive down costs); *see also* Allen, *supra* note 9, at 15 (discussing the controversial use of data mining techniques to identify patients with alcoholism). Another example of how the increasingly extensive use of private medical data is driven by economic concerns is in the pharmacy benefit management ("PBM") industry. Here, companies compile a vast amount of prescription-related information on patients, then analyze it to promote more effective prescription practices by physicians, increased compliance with the drugs' instructions by patients, and use of cheaper drugs by doctors and pharmacists. As a testament to the economic importance of this use of medical records, pharmacy retailer, Rite Aid Corporation, recently acquired Eli Lilly's PBM subsidiary for $1.6 billion, thereby acquiring access to information on 300 million prescriptions annually. *See Rite Aid to Acquire Lilly's PCS Health Systems;*

practice management companies routinely employ staffs of "utilization review experts,"[42] and implement complex information management systems to monitor patient care delivery by collecting private patient data.[43] The collection of private medical data to further these industry-wide cost containment goals is such a large phenomenon that an entire industry has developed to meet the information collection and management needs of providers. According to a research analyst who focuses on health care services, "[t]he health care MIS [(management information systems)] industry has gone from an in-house function at the insurance company to a rapidly growing force with a few dozen players and a few billion [dollars] in revenue."[44]

Because of these changes in the health care industry, private medical information users have become too numerous to catalog. The Institute of Medicine, a leading association of medical professionals,[45] found that the complete list of groups, individuals, and other corporate, research, or government entities authorized to use patient records would encompass all entities affiliated with the health care industry in our country.[46] Furthermore, the installation of database technology to facilitate use of patient information often disregards privacy laws and restrictions; laws are so complex and

---

Pharmacy Benefits Management Subsidiary, BUS. WIRE, Nov. 17, 1998, *available in* LEXIS, News Library, CURNWS File ("The combination brings together two leading companies engaged in enhancing the quality of pharmacy care and in the management and containment of health care costs . . . .").

[42] Interview with Howard Capek, *supra* note 38 (discussing utilization review and explaining that utilization review experts study patient data obtained during the provision of care in an effort to develop cost-saving practice standards and identify over-provision of care by the provider's doctors). "Utilization review" and "utilization management" are terms that encompass the broad range of efforts by health care providers and payors to reduce costs by analyzing practice patterns of doctors, and standardizing these practices. *See, e.g.*, Thomas Bodenheimer & Kevin Grumbach, *The Reconfiguration of US Medicine*, 274 JAMA 85, 86-87 (1995) (discussing insurers' use of utilization review controls and the rise of health maintenance organizations focused on containing costs through some form of utilization management).

[43] *See, e.g.*, Allen, *supra* note 9, at 15 (noting that $2 billion is currently spent each year by companies to build medical record information systems).

[44] Interview with Michael Wiggins, Health Care Investment Banking Associate, Credit Suisse First Boston, in Phila., Pa. (Jan. 28, 1998) (noting the rapid development and growth of the health care management information systems industry).

[45] *See* Michael Fumento, *The Squeaky Wheel Syndrome*, AM. SPECTATOR, Dec. 1998, at 1, 6 (describing "the Institute of Medicine [as] a branch of the highly reputed, nongovernmental National Academy of Sciences").

[46] *See* COMMITTEE ON IMPROVING THE PATIENT RECORD, INST. OF MED., THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE 75 (Richard S. Dick et al. eds., rev. ed. 1997) ("An exhaustive list of patient record users would essentially parallel a list of the individuals and organizations associated directly or indirectly with the provision of health care.").

varied that companies often implement information systems without careful consideration of privacy law.[47] The scale and scope of the information management changes in health care, when coupled with the disparity in the coverage and strength of laws governing the use of private medical records,[48] has contributed to the urgent need for a strong, uniform set of guidelines covering the use of patient information.

B. *HIPAA and the* HHS Report

These and other factors gave rise to a number of federal legislative initiatives that have sought to address the need for such privacy protections. Eventually, Congress passed HIPAA,[49] which sets forth a procedure for the development of such regulations or laws. A discussion of the Act's passage and its content is below, as well as an examination of the resulting *HHS Report*.[50] Finally, an introduction and description of the *Report*'s law enforcement exception follows.

1. The Health Insurance Portability and Accountability Act of 1996

In the face of rapid and profound changes in health information technology and its usage by health care participants, compelling arguments exist for general, federal-level confidentiality protections.[51] Consequently, lawmakers recognized a need for federal legislative action, and there has been

---

[47] Interview with Mark Davidson, *supra* note 34 (explaining the overwhelming lack of understanding about privacy law by health care information technology professionals in general). From a purely doctrinal perspective, the laws may not be terribly complex, but there does exist a daunting amount of legal infrastructure for national medical information users. For instance, the medical information practitioner's *Patient Confidentiality* reference lists state confidentiality and reporting statutes that apply in abortion, AIDS/HIV, and child abuse cases. The applicable laws are rarely found in the same code sections across these three illustrative scenarios, and specific confidentiality rules for each state are often found in yet another area of its statutory framework. *See* JANET MCGEE SAUNDERS, PATIENT CONFIDENTIALITY 56-64 (1996).

[48] *See infra* Part II (providing an overview of the scope of law enforcement access to medical records).

[49] HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.).

[50] HIPAA mandated that HHS draft proposed privacy rules and report to Congress on its proposal. *See id.* § 264(a), 110 Stat. at 2033 (setting forth the role of HHS in this process).

[51] For example, it has been noted that the current patchwork of protections results in "rights [that] have not been uniformly enforced," despite the ability of national insurers to amass, access, and use large amounts of confidential information. Denise M. Nagel, M.D., Director, National Coalition for Patient Rights, Address to the National Committee on Vital and Health Statistics (Feb. 19, 1997) (visited Mar. 26, 1999) <http://www.tiac.net/users/gls/mynameis.htm>.

significant legislative activity in the area of medical records privacy over the past several years.[52]

Although recent attempts to pass legislation in Congress have failed,[53] the enactment of HIPAA put into motion the beginnings of a complete federal legal structure addressing health information privacy.[54] In particular, HIPAA contains some language, albeit limited, that addresses specifically the lack of privacy protections regarding health information.[55] Prior to this, legislators considered it constitutionally appropriate for individual state laws to govern medical records privacy,[56] and consequently a patchwork of state laws currently offers citizens widely disparate levels of protections.[57] Since no concerted effort created this current framework, no uniformity exists among the states' laws.[58]

---

[52] *See, e.g.*, Gilbert, *supra* note 32, at 94-95 (listing recent congressional legislative initiatives). "There have been many attempts in the past several years to enact federal legislation that addresses the protections of health information privacy." *Id.*; *see also* LOWRANCE, *supra* note 37, at 60-61 (mentioning briefly the "[s]everal Federal bills governing medical privacy . . . [that] have been proposed in the past few years"). For a comprehensive overview of the legislative activity prior to HIPAA, see Bartley L. Barefoot, Comment, *Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline?*, 77 N.C. L. REV. 283, 310-14 (1998).

[53] *See* Gilbert, *supra* note 32, at 94 (noting that all five medical records privacy bills introduced in the 104th Congress failed to be enacted); Barefoot, *supra* note 52, at 310 ("Despite widespread agreement with the fair information principles [espoused in a 1973 federal report on confidentiality], repeated attempts to enact a federal health confidentiality law have been unsuccessful.").

[54] *See* Allen, *supra* note 9, at 13-14 (noting that HIPAA represents a first step toward a complete legal structure).

[55] *See* HIPAA § 262, Pub. L. No. 104-191, 110 Stat. 1936, 2021 (1996) (codified in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.) (requiring security standards or safeguards to ensure the integrity and confidentiality of health information and to protect against unauthorized uses). Note, however, that this language is limited in scope and purpose. *See infra* notes 59-72 and accompanying text (discussing the scope of privacy protection that is provided indirectly by HIPAA).

[56] For example, in discussing the States' authority to make laws regarding health information privacy, Françoise Gilbert plainly notes that in the past, "[t]hese matters were considered to be local in nature. The Tenth Amendment to the United States Constitution clearly grants each state the power to legislate health care issues, including the protection of medical records privacy." Gilbert, *supra* note 32, at 93.

[57] *See infra* text accompanying note 95 (noting that the *HHS Report* declares that current state protections are inadequate).

[58] Montana and Washington are the only two states thus far to enact the 1985 Uniform Health Care Information Act, despite the fact that it is a model act. *See* MONT. CODE ANN. §§ 50-16-501 to 50-16-553 (1995); WASH. REV. CODE ANN. §§ 70.02.005-70.02.904 (West 1992 & Supp. 1993).

Interestingly, HIPAA does not list among its purposes the establishment of strong privacy safeguards.[59] Instead, the intention of the Act is to improve health insurance coverage portability and renewability, and make changes to medical savings accounts and other tax-related health care payment issues.[60] Title II of the Act, where the HHS mandate resides, addresses fraud prevention and requires simplification of health claim administration.[61] In particular, Subtitle F of Title II deals with administrative simplification; its goal is to improve the administration of the Medicare and Medicaid programs and "the efficiency and effectiveness of the heath care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[62] Most importantly, section 262 of HIPAA focuses on the enactment of standards for the secure transmission of health information data.[63] Some legal commentators view this section of the law as currently representing the best foundation for appropriate and substantial health information privacy protection at the federal level.[64]

HIPAA, and in particular section 262, does not provide direct protection of individual health information privacy. Rather, the law establishes a framework and series of deadlines for the creation of more specific laws or regulations. First, HIPAA establishes the scope of data standards, the definition of those standards, and to whom and to which transactions the standards will apply.[65] With respect to these standards, section 262 requires the adoption of "safeguards to ensure the integrity and confidentiality of the information and protect against threats to security or integrity of the information and unauthorized uses of the information."[66] Instead of providing fur-

---

[59] *See* 42 U.S.C. § 242k (1994 & Supp. II 1996) (identifying the purpose of the Act as improvement of the Medicare program, the Medicaid program, and the "efficiency and effectiveness of the health care system"); *see also id.* § 1320d to d-8 (Supp. II 1996); *id.* § 1395cc (1994 & Supp. II 1996).

[60] *See id.* § 1320d to d-8 (amending ERISA and the Public Health Service Act with respect to availability, portability, and renewability of health insurance coverage).

[61] *See id.* (creating standards for communications, as well as fraud and abuse prevention).

[62] HIPAA, Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021 (1996).

[63] *Id.* § 262 (establishing universal participant identifiers and authentication standards).

[64] *See, e.g.*, Gilbert, *supra* note 32, at 95 ("To date, [section] 262 appears to be the piece of legislation that is the most able to provide some guidance and relief in framing an adequate protection for health care information.").

[65] *See* 42 U.S.C.A. § 1320d (defining "code set," "health care clearinghouse," "health care provider," "health information," and "health plan" for purposes of the Act). These types of standards are intended to create more uniformity among medical data, facilitating transmission of data from one user to another throughout the health care delivery system.

[66] *Id.* § 1320d-2(d).

ther specificity, section 262 requires the HHS Secretary to adopt security standards that consider current technical information system capabilities, the cost of security measures, the need for training those with access to health information, the value of audit trails in computerized record systems, and the needs and capabilities of small or rural health care providers.[67]

Finally, the Act states that within twelve months of its enactment, the HHS Secretary must submit "detailed recommendations" to Congress "on standards with respect to the privacy of individually identifiable health information."[68] Moreover, if Congress fails to enact legislation governing standards with respect to the privacy of individually identifiable health information within thirty-six months after the passage of HIPAA, the HHS Secretary must promulgate final regulations containing such standards no later than forty-two months after the passage of HIPAA.[69] Thus, in the event Congress fails to pass a health information privacy law by August 1999, HIPAA mandates that HHS must establish federal regulations, with the original *HHS Report* serving as the foundation for such regulations.[70]

HIPAA is the first crucial step toward federal health records privacy, yet it is a hesitant one.[71] The Act's primary focus is on health information standardization, not privacy, and it does not create immediate safeguards against unwarranted intrusions.[72] Legal commentators consider parts of the

---

[67] *See id.* § 1320d-2(a)(1) (requiring the HHS Secretary to consider various factors when establishing standards for electronic exchange of health information and standard unique health identifiers).

[68] HIPAA § 264, 110 Stat. at 2033.

[69] *See id.*; *see also* Allen, *supra* note 9, at 13 (outlining HIPAA's deadlines for regulatory and legislative action).

[70] *See* HIPAA § 264, 110 Stat. at 2033. There seems to be ample political impetus for congressional resolution of HIPAA's requirements, *see, e.g.*, Lee Bowman, *Congress to Try Again for New Medical-Records Privacy Law*, HOUS. CHRON., Dec. 26, 1998, at A6 (noting Congress's desire to craft a legislative solution and its antipathy toward the *HHS Report*'s proposals), and legislators have put forth multiple proposals, *see* Barefoot, *supra* note 52, at 319-21 & n.258 (describing in detail the legislative initiatives pertaining to the HIPAA deadline for a new privacy law). Privacy commentators, however, are not sanguine about Congress's prospects for achieving a legislative solution. *See, e.g.*, *id.* at 284 ("If the past serves as any indication, disagreements on several key issues may cause the deadline to pass without congressional action.").

[71] One commentator characterized the inclusion of privacy protections within HIPAA as follows: "One goal of that legislation [(HIPAA)] was to speed the computerization of health care records, and privacy advocates inserted language to ensure that computerization was accompanied by better protection." Allen, *supra* note 9, at 13.

[72] *See supra* note 59 and accompanying text (noting that HIPAA does not list among its purposes the establishment of strong privacy safeguards).

Act, however, to be a positive first step toward stronger safeguards.[73] To this end, its call for an HHS proposal of rules is the most concrete initiative Congress has undertaken, and the resulting *HHS Report* addresses many of the privacy concerns that arise in a modern, information-age health care delivery system.

2. The *HHS Report*

The resulting *HHS Report*, entitled *Confidentiality of Individually-Identifiable Health Information*, is presented in three major sections.[74] It begins with an introduction, which includes a listing and elucidation of the principles behind the *Report*'s recommendations.[75] Next, a recommendations section provides guidance on the scope of, requirements for, and exceptions to the general protections discussed.[76] Lastly, a concluding remarks section briefly reviews the main thrust of the *Report*.[77] Not surprisingly, various interest groups expressed dissatisfaction with certain details in the *Report*, but on the whole, many privacy advocates and health care delivery industry representatives felt that the *Report* was balanced and fair, despite these perceived flaws.[78] A brief overview of the *Report* follows.

The *Report* begins by underscoring the need for federal legislation and acknowledging that current state and federal protections are inadequate, especially in light of the rapid technological changes sweeping through health care data use.[79] It then discusses five principles which serve as a framework for the remainder of the *Report*: (1) appropriate boundaries that prevent information flow for non-health reasons, such as firing an employee; (2) secu-

---

[73] *See* Allen, *supra* note 9, at 13 (noting that, as a result of HIPAA, Congress will probably pass a federal privacy law aimed at "limiting the authorized uses of medical information and providing for legal redress in the event of abuse").

[74] *See* HHS REPORT, *supra* note 18.

[75] *See id.* pt. I.

[76] *See id.* pt. II.

[77] *See id.* pt. III.

[78] *See, e.g.*, *HHS Privacy Plan Due This Week*, *supra* note 19, at 1, (citing approval from the Health Information Management Association, for example). Note, however, that one reason the *Report* may not have drawn so much criticism is that some observers felt the *Report* was too general to be controversial. They argued that the Clinton administration abdicated its responsibility to develop a detailed draft law governing medical records privacy. *See, e.g.*, Jerry Geisel, *Administration Leaves Rules on Record Privacy to Congress*, BUS. INS., Sept. 22, 1997, at 2 (arguing that the Clinton Administration privacy guidelines are "general" and "vague" and noting that the "Clinton Administration will leave it to Congress to develop new rules governing the privacy of medical records").

[79] *See* HHS REPORT, *supra* note 18, pt. I.B (arguing that "[t]he existing legal structure does not effectively control information about individuals' health").

rity to prevent insurers and marketers from abusing the data; (3) consumer controls to allow people to check their records for mistakes and to find out who else has looked at them; (4) accountability so records abusers are punished; and (5) public responsibility, allowing adequate access to the research and teaching communities.[80] The first four of these principles undergird the *Report*'s recommendations, which protect individuals' private health information. For example, the impetus driving the first principle, the recognition of appropriate boundaries, is described by HHS Secretary Donna Shalala as follows:

> [Drawing appropriate boundaries] means hospitals can use this information to provide and pay for quality care for their patients. And, subject to the requirements of other laws such as the Americans with Disabilities Act of 1990, employers could use it to provide on-site care for their employees or to administer a self-insurance plan. But, those same employers should not be able to use information obtained for health care purposes to make decisions about job hiring and firing, placements and promotions. We are recommending strong protections for Americans from the inappropriate disclosure of their medical records.[81]

Hence, the *Report* draws a strict line between proper and improper uses of health data, using a "for health-related purposes" only rule. Applying this guiding principle, specific proposals result concerning those covered by the recommendations, the information uses permitted, and the types of information covered.[82] Similarly, recommendations also logically follow from the next three principles: standards for security measures are the result of the security principle;[83] rights of individuals to review their own health data come from the notion that consumer controls should be in place;[84] and suggested penalties arise from the concept that abusers of private health data should be punished.[85]

The fifth principle, the so-called "public responsibility" principle, stands in stark contrast to the other foundations of the *Report* (and their consequent recommendations). In essence, this notion of public responsibility

---

[80] *See id.* pt. I.E—I.I.

[81] *Protecting Our Personal Health Information: Privacy in the Electronic Age: Hearings of the Senate Comm. on Labor and Human Resources*, 105th Cong. 21 (1997) (statement of Donna Shalala, Secretary of Health and Human Services) [hereinafter *Hearings Statement*].

[82] *See* HHS REPORT, *supra* note 18, pt. II.A (describing suggestions for coverage of a federal health privacy statute).

[83] *See id.* pt. II.B(2) (recommending "appropriate levels and types of protective measures").

[84] *See id.* pt. II.C(2) ("The ability to see one's own record is central to effective control of information and is a basic fair information practice.").

[85] *See id.* pt. II.H (describing civil and criminal penalties to aid enforcement of privacy law).

seems to be a caveat to the general protections that the *Report* seeks to establish. This caveat leaves open the door to privacy intrusion in the sphere of personal medical information, and implicitly acknowledges that the proposal does not intend to create absolute privacy rights regarding one's medical history. Secretary Shalala describes this idea as follows:

> These four principles—Boundaries, Security, Consumer Control and Accountability—must be weighed against the fifth principle, Public Responsibility.
>
> . . . .
>
> Just like our free speech rights, privacy rights can never be absolute. We have other critical—yet often competing—interests and goals. We must balance our protections of privacy with our public responsibility to support national priorities—public health, research, quality care, and our fight against health care fraud and abuse.
>
> As a major payer of health care in this country, our Department is acutely aware of the need to use health records to fulfill those responsibilities.[86]

It is the fifth principle which serves as the justification for the law enforcement exception. This exception is discussed in the following Section.

3. The *HHS Report*'s Law Enforcement Exception

As the discussion above demonstrates, much of the reasoning behind the *Report*'s recommendations is centered on the need for laws that will protect individual health information privacy in the face of the rapid technological changes and computerization of medical records. This attitude is clear from the plain language in HIPAA's section 262[87] and the stated intentions of the *Report*. For example, the *Report* asserts that

> as the health care system becomes more integrated and more computerized, it is becoming difficult to determine the appropriate person or place where our health information can be accessed or controlled.
>
> For th[is and other] reasons, [HHS is] recommending that Congress replace the ineffective use of authorizations with a system of Federal legislative controls on the use of health information collected by health care payers and providers.[88]

Moreover, during her testimony, Secretary Shalala argued for a national standard for confidentiality,[89] and stressed that the *HHS Report*'s recom-

---

[86] *Hearings Statement*, *supra* note 81, at 23.

[87] *See supra* note 63 and accompanying text (noting that section 262 of HIPAA focuses on the need to protect the security of electronic health information).

[88] HHS REPORT, *supra* note 18, pt. I.B.

[89] *See Medical Records: HHS Proposes Privacy Standards*, HEALTH LINE, Sept. 12, 1997, at 1, 1 ("[Shalala] said that 'by establishing a basic national standard of protection there

mendations for new, strong federal standards represented a needed response to what she described as "revolutions in biology, communications, and health care."[90] Shalala emphasized the need for standardized and stringent national protections with a "fundamental" rhetorical question: "Will our health records be used to heal us or reveal us? The American people want to know. As a nation, we must decide."[91] Curiously, however, this attitude did not justify a federal standard governing law enforcement's use of private medical records. Despite the fact that the rapid computerization of health records ostensibly could also facilitate previously unimagined and inappropriate usage by law enforcement,[92] HHS chose to leave this area of medical records privacy untouched.[93]

Further, the reasoning for this unusual treatment seems at odds with another premise underlying the *Report*'s call for federal-level standards—the incomplete and inconsistent nature of the "patchwork of State health privacy laws."[94] The *Report* declares that current state protections are inadequate, and that because state laws "vary greatly in scope and strength, . . . the situation has been described as 'a morass of erratic law, both statutory and judicial, defining the confidentiality of health information.'"[95] However,

---

will be clear guidance and significant incentives for the fair treatment of personal information . . . .'").

[90] *Hearings Statement*, *supra* note 81, at 25.

[91] *Id.* at 20.

[92] *See, e.g.*, *infra* notes 224-26 and accompanying text (discussing potential law enforcement abuse in a situation where HHS workers inadvertently discover criminal activity while reviewing medical records for other purposes).

[93] One reason this may have occurred is that Secretary Shalala bowed to pressure from the Department of Justice, which was eager to protect law enforcement's easy access to private medical records. *See Privacy Proposals Include Controversial Surprises*, HEALTH DATA MGMT., Oct. 1997, at 1, 1 ("Capitol Hill insiders say Shalala lost a battle with the Justice Department over the law enforcement/intelligence provisions.").

[94] HHS REPORT, *supra* note 18, pt. I.J.

[95] *Id.* pt. I.B (quoting WORKGROUP FOR ELECTRONIC DATA EXCHANGE, REPORT TO THE SECRETARY OF U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES app. 4, Confidentiality and Antitrust Issues 5 (1992)). The *HHS Report* is hardly the first authority to reach this conclusion. *See, e.g.*, LAWRENCE O. GOSTIN ET AL., ELECTRONIC PRIVACY INFORMATION CTR., LEGISLATIVE SURVEY OF STATE CONFIDENTIALITY LAWS, WITH SPECIFIC EMPHASIS ON HIV AND IMMUNIZATION, REPORT TO THE U.S. CENTERS FOR DISEASE CONTROL AND PREVENTION ET AL., pt. 4, § VIII.A (1996) (last modified Mar. 1, 1999) <http://www.epic.org/privacy/medical/cdc_survey.html> (noting that "[l]aws protecting the confidentiality of health care information vary markedly from state to state," and describing the problems this causes for patients' privacy rights and other issues it raises for various interested parties in the health care delivery system). Indeed, this 1996 legislative survey noted with alarm the high degree of variation of statutory protection afforded by the contradictions in the legal frameworks within individual states. *See id.* at pt. 4, § IV (noting that states' laws are often internally inconsistent, conferring varying degrees of privacy protection to different types of information, and adopting inconsistent approaches to different state government

this diverges sharply from Secretary Shalala's assertion that current law enforcement access to private medical records operates within a set of "well-established procedures of the criminal justice system."[96] As Part II of this Comment shows, few, if any, legal commentators would share Secretary Shalala's belief that the laws and cases addressing law enforcement's use of private medical information are well-defined.[97]

The *Report*'s recommendations concerning law enforcement's access to private medical records, however, reflect Secretary Shalala's sentiments. Simply put, the *Report* proposes making no changes to the existing legal landscape regarding law enforcement use of medical records. On more than one occasion, the *Report* notes that its authors "are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies."[98] Instead, its goal is much less ambitious, recommending "that the [*Report*'s proposed] legislation maintain current practices by permitting disclosure of health information to law enforcement authorities."[99]

The *Report*, however, does recommend a solution for improper privacy violations that may arise in the law enforcement exception context: punish wrongdoers. The *Report* suggests penalties for the inappropriate use of private medical information.[100] Both the *Report* and Secretary Shalala's testimony before Congress make clear that these penalties should apply equally to law enforcement representatives and any other information abusers.[101]

---

practices and protocols concerning public health information). Such findings have led Robert Gellman to observe that state-level frameworks result in "a legal, political and practical mess." Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level?: Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 137 (1996).

[96] *Hearings Statement*, *supra* note 81, at 24.

[97] Indeed, Secretary Shalala herself seems conflicted on this matter. During her congressional testimony, she stated:

> If a law enforcement officer in this country does find other criminal activity, there are other laws that affect how they can use that information and the courts have spoken on that subject, *sometimes in inconsistent ways*. . . . [B]ut I think the important thing is that we believe that there are laws that restrict *and clarify* what law enforcement officers do in terms of their access.

Id. at 9 (emphasis added). It is difficult to grasp how *inconsistent* judicial results can lend *clarity* to law enforcement action in these matters.

[98] HHS REPORT, *supra* note 18, pt. II.E(9).

[99] *Id.* pt. II.E(10).

[100] *See id.* pt. II.H (recommending civil and criminal penalties for violations of confidentiality of health information).

[101] *See Hearings Statement*, *supra* note 81, at 9-10 ("[A] law enforcement officer who acted in an inappropriate way—who did not have a justification for going to look at someone's medical record, would be subject to criminal penalties, including jail as well as fines.");

This solution seems overly simplistic, however, especially when compared with the more comprehensive, principled approach taken in the overwhelming majority of the *Report*. A host of logical and practical flaws seem possible given this superficial treatment of the law enforcement exception issues.[102]

There is no doubt that there exists a logical tension between the rationale, approach, and resulting recommendations related to the law enforcement exception on the one hand, and the balance of the *Report* on the other. To a certain extent, this is unavoidable. Despite the fact that it runs counter to the other four principles guiding the *Report*, at its core the fifth principle of public responsibility seems justified and acceptable—law enforcement must have a defined exception to the general rule that health records can only be used for health-related purposes. It is the *Report*'s treatment of this principle, more than the principle itself, that contradicts the spirit and reasoning of the *Report*'s other recommendations. Just as the changes in health information usage and database technology justify a reevaluation of the laws governing such usage, it seems logical that the law enforcement exception in this area of medical records privacy could also benefit from review and standardization. The balance of this Comment will review current law to test the *Report*'s assertion that the exception is well-defined, and to determine whether current legal standards appropriately protect individuals' privacy interests in light of the profound technological changes—something that is assumed by the recommendations of the *Report*. Additionally, this Comment suggests and defends some possible improvements in the *Report*'s stance on law enforcement use of medical records.

II. LEGAL BACKGROUND OF THE LAW ENFORCEMENT EXCEPTION TO MEDICAL RECORDS PRIVACY

If the *Report* accepts the current state of the law enforcement exception, then it seems logical to review the present legal frameworks of the exception in order to determine if they sufficiently protect individual medical records privacy. In general, the exceptions represent a patchwork structure, as the *Report* concedes when assessing medical records privacy law in general.[103] The sprawling nature of the law, however, does not mean that all of the developments are hostile to individuals' medical records privacy rights

---

HHS REPORT, *supra* note 18, pt. II.E(10) ("[O]ur recommendations would make obtaining health information under false pretenses be a Federal felony.").

[102] For a critique of the *Report*'s stance, see *infra* Part III, which outlines arguments for strengthening the law enforcement exception of the HHS proposal.

[103] *See supra* note 95 and accompanying text (describing the confusion of varying state statutory and judicial medical privacy laws).

with respect to law enforcement use; indeed some strong statements and hopeful interpretations exist.[104] This Part briefly outlines the possible interpretations of the current law regarding the law enforcement exception. First, it discusses two constitutional issues: the existence of a constitutional right to medical records privacy independent of the Fourth Amendment, and the extent of the Fourth Amendment protection against medical record searches and seizures. Next, it reviews applicable federal laws. Finally, it considers the relevant issues in state law, including both state statutes and case law regarding potential protections.

A. *An Independent Constitutional Right to Privacy*

Although the Fourth Amendment prohibition against unreasonable searches and seizures may create the most likely source of constitutional protection against wrongful law enforcement access to private medical records, other constitutional protections also exist. This Subpart provides a brief history of the judicial evolution of these protections. First, it offers insight into the growth and development of non-Fourth Amendment protections for medical records privacy. Second, it examines later cases that appear to restrict or undercut these potential protections in the medical records area.

1. The History and Developments of Penumbral Privacy Rights

The U.S. Supreme Court has recognized a constitutional right to privacy independent of the protections afforded by the Fourth Amendment.[105] The

---

[104] *See, e.g.*, *infra* notes 123-28 and accompanying text (discussing the penumbral constitutional privacy protections implied by the *Whalen v. Roe* decision); *infra* note 149 and accompanying text (citing cases that support a Fourth Amendment basis for medical records privacy protections); *infra* notes 170-71 and accompanying text (approving of the analytical framework of protection espoused in *Katz v. United States*, and demonstrating HIPAA's consistency with this framework); *infra* notes 184-90 (discussing the privacy protections included in the Freedom of Information Act applicable to medical records held by the government); *infra* notes 195-206 (describing tort- and contract-based common law protections against improper medical records use and/or disclosure).

[105] *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973) (finding that a state law prohibiting abortion under any circumstances except to save the life of the mother was an unlawful invasion of an individual's constitutional, non-Fourth Amendment privacy rights); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (using penumbral privacy rights to invalidate a state law prohibiting the distribution of contraceptives to unmarried individuals); Stanley v. Georgia, 394 U.S. 557, 559 (1969) (striking down a state statute prohibiting sexually obscene material in a private residence using non-Fourth Amendment privacy right justifications); Loving v. Virginia, 388 U.S. 1, 12 (1967) (invalidating a state statute barring interracial marriage using non-Fourth Amendment privacy rights reasoning); Griswold v. Connecticut, 381 U.S. 479,

relevant cases, although rarely touching on the specific issue of medical records privacy, do address squarely the fundamental issue of government intrusion into personal information.[106] Medical records surely fall into this category.[107] This line of cases really begins with an idea presented in a landmark law review article entitled *The Right to Privacy*, written by Samuel Warren and Louis Brandeis.[108] Warren and Brandeis argued that there should exist an individual right to privacy, even where the harm is solely intangible, such as harm to one's feelings.[109] Presaging the justifications for the current *HHS Report*, the authors argued that technological advances such as cameras and high-speed newspaper printing presses "have invaded the sacred precincts of private and domestic life."[110] This right was not a mere property right, such as an interest in one's personal papers or letters.[111] Rather, it protected the underlying intellectual product, which arose from the solace of preventing public disclosure of such information.[112]

Far removed in time from this foundation, *Griswold v. Connecticut*[113] was the first case that sought to develop an implicit constitutional right of

485 (1965) (holding that various constitutional "penumbral rights" exist to provide privacy protection and render a state law forbidding the use of contraceptives unconstitutional).

[106] *See, e.g., Roe*, 410 U.S. at 154 (concluding "that the right of personal privacy includes the abortion decision" and limits government intrusion into this decision); *Eisenstadt*, 405 U.S. at 453 (holding that the right of privacy extends to an individual's right to be free from "unwarranted government intrusion" when making personal decisions such as "whether to bear or beget a child"); *Stanley*, 394 U.S. at 566 (noting that it is impermissible for the government to premise legislation on controlling the private information contained in "a person's private thoughts"); *Griswold*, 381 U.S. at 484 (noting that "[v]arious [penumbral] guarantees create zones of privacy" protected from government intrusion).

[107] Even cases generally hostile to privacy interests in medical records concede this point. *See, e.g.*, Doe v. Southeastern Pa. Transp. Auth. (SEPTA), 72 F.3d 1133, 1137 (3d Cir. 1995) (recognizing that there exists a presumptive constitutional privacy right in one's medical records).

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

[109] *See id.* at 197-99 & n.1 (arguing that a general right to privacy affords a remedy for mental pain).

[110] *Id.* at 195.

[111] *See id.* at 201 ("What is the thing which is protected? Surely not the intellectual act of recording . . . but that fact itself. It is not the intellectual product, but the domestic occurrence.").

[112] *See id.* at 201-05 ("[T]he protection afforded to thoughts, sentiments, and emotions . . . so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone.").

[113] 381 U.S. 479 (1965) (holding that a Connecticut law forbidding the use of contraceptives unconstitutionally intruded upon the right of marital privacy).

privacy independent of the Fourth Amendment.[114] *Griswold* signaled an analytical shift from the Fourth Amendment cases' rights-based approach toward a broader interpretation of constitutional interests. It balanced these interests against the interests of government.[115] Some commentators have argued that as a result of this shift in reasoning, "the clear trend has been the expansion of privacy rights."[116] Although the Court in *Griswold* issued four separate opinions in defense of its judgment, the ruling demonstrated that there existed a privacy right distinct from the Fourth Amendment.[117] Later cases, such as *Loving v. Virginia*,[118] *Stanley v. Georgia*,[119] and *Eisenstadt v. Baird*,[120] upheld and invigorated the privacy rights of individuals. Each case recognized a legitimate constitutional privacy right by weighing that right against the governmental interests in limiting or intruding upon it.[121] In *Roe v. Wade*, the Court concluded that the balance weighed against the state's interest in protecting potential life by banning abortions.[122] *Roe* served as a strong statement in support of the privacy right and its relative weight when compared to governmental interests.

---

[114] *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 21 (1997) (arguing that *Griswold* began the "trend [toward] the expansion of privacy rights").

[115] *See id.* (discussing the Court's shift toward "a utilitarian cost-benefit analysis which balances the costs to privacy and the benefits to public safety").

[116] *Id.* DeCew argues convincingly that the reasoning in *Griswold* was anticipated by similar constitutional arguments protecting privacy in the Georgia case, *Pavesich v. New England Life Insurance Co.*, 50 S.E. 68 (Ga. 1905). *See* DECEW, *supra* note 114, at 23 (discussing the "natural basis for connecting the two cases").

[117] 381 U.S. at 485 (noting the validity of "penumbral rights of 'privacy and repose'" (citation omitted)).

[118] 388 U.S. 1, 2 (1967) (striking down a Virginia statute outlawing interracial marriage based on the Court's recognition of a penumbral privacy right).

[119] 394 U.S. 557, 559 (1969) (citing a penumbral privacy right as an important justification for allowing obscene materials in an individual's home).

[120] 405 U.S. 438, 443 (1972) (citing a penumbral privacy right as the rationale for allowing distribution of contraceptive devices).

[121] *See, e.g.*, *id.* at 453 (supporting a right to marital privacy, including the use of contraception); *Stanley*, 394 U.S. at 567 (supporting a right to private possession of obscene matter); *Loving*, 388 U.S. at 12 (supporting a right to marry interracially).

[122] 410 U.S. 113, 150, 162-63 (1973) (acknowledging a state interest in protecting potential life, but concluding that this interest does not outweigh completely the privacy right of the mother). Note, however, that since *Roe*, the Court has issued numerous opinions that resolve this general balancing in favor of the governmental intrusion. *See, e.g.*, Planned Parenthood v. Casey, 505 U.S. 833, 887 (1992) (finding that Pennsylvania's informed consent restrictions on abortion rights did not impose an undue burden on the individual's constitutional privacy rights espoused in *Roe*); Webster v. Reproductive Health Servs., 492 U.S. 490, 507 (1989) (finding that a state's interest in promulgating a law banning public employees from performing nontherapeutic abortions in public facilities outweighed the individual's constitutional interest); Bowers v. Hardwick, 478 U.S. 186, 196 (1986) (upholding a Georgia statute criminalizing sodomy).

With these developments as a foundation, the Supreme Court in *Whalen v. Roe* issued its most comprehensive definition of the privacy right thus far, by acknowledging both an "individual interest in avoiding disclosure of personal matters" and an "interest in independence in making certain kinds of important decisions."[123] This case is of particular relevance in the medical records privacy arena since it involved the constitutionality of a New York law mandating centralized computer record keeping of prescriptions for specific addictive, but lawful, drugs, complete with patient-identifiable information.[124] Although the Court upheld the statute at issue,[125] the case is encouraging for a number of reasons. First, the Court recognized a more comprehensive privacy right (including an "interest in avoiding disclosure of personal matters") that could encompass one's right to avoid law enforcement intrusion into personal medical information.[126] Second, the Court's balancing focused heavily on the potential harms caused by the collection and maintenance of such a database; only after the Court was satisfied that the privacy risks were obviated did it acknowledge the state's interest in collecting such data.[127] Finally, Justice Brennan's concurrence recognized that the accessibility of the data was troubling, and indicated that future technological developments might create the need to revisit this balancing and to restrict the government's use of technology that would place privacy rights at risk.[128] Although the result of the Court's decision in *Whalen* might seem to limit the potency of this penumbral right in the area of law enforcement's use of medical records, the case at least established that such a right might outweigh similar governmental intrusions into personal health information in the future.

---

[123] 429 U.S. 589, 599-600 (1977).

[124] *See id.* at 591 (addressing "whether the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market").

[125] *See id.* at 603-04 (finding that the potential privacy threats inherent in New York State's Controlled Substances Act did not rise to an unconstitutional "invasion of [privacy] right[s] or libert[ies]").

[126] *Id.* at 599.

[127] *See id.* at 593-94 (finding that protections such as locking the data tape in a storage facility when not in use, running the data off-line, and providing access to only a limited number of officials were sufficient to ensure confidentiality).

[128] *See id.* at 607 (Brennan, J., concurring) ("I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

2. Post-*Whalen*: Developments Limiting the Scope of a Constitutional Right to Medical Records Privacy

Commentators have severely criticized the penumbral right of privacy since its inception because it is not explicitly stated in the Constitution, and because courts have asserted it in a vast array of cases.[129] Since the *Whalen* decision, the Supreme Court has been more reluctant to invigorate the privacy interests of individuals in the medical records context. Two cases in particular illustrate the judicial balancing framework and ultimate lessening of privacy interests in health information.[130] These cases provide essential insight into the potential value of this independent constitutional right in the law enforcement context.

Despite *Whalen*'s cautionary language against doing so, lower courts have read the *Whalen* decision as severely limiting the right to informational privacy, thereby shifting the balance strongly in favor of governmental interests. According to the Third Circuit in *United States v. Westinghouse*, a court should analyze seven factors to determine the extent of this constitutional privacy right: (1) the type of record requested; (2) the information the record 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 (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest favoring access.[131] The *Westinghouse* court considered a scenario closely analogous to the law enforcement use of private medical records. In that case, the federal government, through the National Institute for Occupational Safety and Health ("NIOSH"), served a subpoena on Westinghouse for employees' medical records in connection with an investigation concerning a possible workplace hazard.[132] The court concluded that the subpoena was valid, approving the governmental interest

---

[129] *See, e.g.*, Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967) (criticizing the early penumbral privacy rights cases).

[130] *See* Doe v. Southeastern Pa. Transp. Auth. (SEPTA), 72 F.3d 1133, 1135 (3d Cir. 1995) (finding that the employer's need to access prescription records outweighed the employee's privacy interest in a case in which an employer discovered that an employee had AIDS based on the employee's drug purchases made through the employee health plan); United States v. Westinghouse, 638 F.2d 570, 580 (3d Cir. 1980) (finding that employees' constitutional privacy rights were not sufficient to overcome a governmental demand for their confidential medical records for investigatory purposes); *see also infra* notes 134-42 and accompanying text (discussing the *Doe* and *Westinghouse* cases).

[131] *See Westinghouse*, 638 F.2d at 578 (setting forth the analysis to determine the extent of a privacy right).

[132] *See id.* at 573 (discussing NIOSH's investigation of Westinghouse's Trafford plant).

in NIOSH's investigatory efforts despite simultaneously recognizing the sensitive and personal nature of the information.[133] It is important to note the level of deference given to the governmental agency and its aims. This is especially important in the law enforcement context, because NIOSH acted as an investigatory body in this instance.

The Third Circuit in *Doe v. Southeastern Pennsylvania Transportation Authority*[134] emphasized the shift away from informational privacy rights and toward valid governmental interests. This case also involved a government entity, SEPTA, in its role as both employer and investigatory body. Here, the plaintiff Doe brought an action under 42 U.S.C. § 1983[135] against SEPTA when he discovered that his employer obtained his confidential medical records as a part of its effort to monitor the use and potential abuse of its prescription drug plan.[136] The court, considering the *Westinghouse* factors, upheld SEPTA's right to collect and monitor such data for these purposes, showing deference to the government even where individually-identifiable patient information was collected improperly.[137] The court noted that "[s]elf-insured employers have the same rights as [government insurers and providers like Medicare and Medicaid],"[138] which routinely obtain and investigate similar data. It acknowledged that, although many of the factors weighed in favor of Doe's privacy rights, the seventh *Westinghouse* factor (relating to the public interest in intrusion) outweighed them.[139] This result, and other cases supporting similar conclusions regarding the penumbral informational privacy right,[140] have caused at least one com-

---

[133] *See id.* at 578-80 ("[W]e believe that the strong public interest in facilitating the research and investigations of NIOSH justify this minimal intrusion into the privacy which surrounds the employees' medical records . . . .").

[134] 72 F.3d 1133, 1135 (holding that a government employer's need for access to employee prescription records for investigative purposes outweighed the employee's interest in confidentiality).

[135] *See* 42 U.S.C. § 1983 (1994) (encompassing and promulgating civil rights protections).

[136] *See Doe*, 72 F.3d at 1135-36 (discussing the rationale behind SEPTA's review of Rite-Aid's prescription drug utilization reports).

[137] *See id.* at 1143 (reversing the district court's judgment and remanding for entry of judgment for the defendants as a matter of law).

[138] *Id.* at 1141.

[139] *See id.* (discussing the employer's "legitimate need for monitoring the costs and uses of their employee benefit programs"). Judge Lewis's opinion in *Doe* points out this relative weighing in succinct fashion. *See id.* at 1147 (Lewis, J., concurring and dissenting) ("[T]he majority places a disproportionate emphasis on factor seven [(the public interest in disclosure)], so much so that the remaining elements of the balancing test [(the individual's privacy interests)] become practically irrelevant to its analysis.").

[140] Lawrence Gostin has observed that "[i]ndividuals asserting a constitutional right to informational privacy are unlikely to obtain a remedy save in cases where the State fails to assert any significant interest or is particularly careless in disclosing highly sensitive informa-

mentator to note that when a "policy development on health information pays some attention to privacy and security concerns, the government is likely to prevail."[141] Thus, when courts employ a flexible balancing approach and the government can assert some legitimate purpose, many privacy interests appear insufficient to overcome the courts' deference to the State.

Whalen set the Court's deferential tone in considering the weight accorded to governmental activities when it observed that numerous state actions "require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[142] As *Westinghouse* and *Doe* demonstrate, this deference has become almost impossible to overcome in the balancing framework typically used when courts consider the penumbral informational privacy right. It seems likely that almost any police action intruding upon private medical records would currently survive such judicial review.

B. *The Fourth Amendment Cases*

The purpose of this Subpart is not to review the vast body of Fourth Amendment law in general, but instead to demonstrate the unresolved and imperfect nature of search and seizure law in the confidential medical records context.[143] First, this Subpart presents cases both undercutting and supporting a right to medical records privacy in the law enforcement context. Second, this Subpart discusses some basic critiques of the reasoning underlying these cases.

1. Ambivalence in the Case Law

An illustrative case that limits individuals' medical records privacy and expands law enforcement's use of such information is *People v. Perlos*.[144] In this case, several defendants were involved in automobile accidents as

---

tion." Gostin, *supra* note 8, at 498 n.211. Gostin cites three recent cases to support this statement. *See id.* (citing *Doe v. Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990), *Woods v. White*, 689 F. Supp. 874 (W.D. Wis. 1988), and *Carter v. Broadlawns Medical Center*, 667 F. Supp. 1269 (S.D. Iowa 1987), to support the proposition that only a complete absence of state interest will allow individual privacy rights to prevail).

[141] *Id.* at 498 (noting that courts allow states wide latitude in protecting and monitoring public health).

[142] Whalen v. Roe, 429 U.S. 589, 605 (1977).

[143] An excellent and comprehensive overview of Fourth Amendment law, however, can be found in 1 JOHN WESLEY HALL, JR., SEARCH AND SEIZURE (2d ed. 1991).

[144] 462 N.W.2d 310, 323 (Mich. 1990) (holding that a state statute requiring hospital personnel to report blood alcohol test results to prosecutors without a warrant does not violate constitutional search and seizure protections).

drivers, and when taken to the hospital for treatment, doctors performed tests on their blood to measure alcohol content.[145] Health care providers turned over the results of these tests to law enforcement pursuant to a state statute which required that the health care provider giving treatment "shall disclose the results of the analysis" to appropriate law enforcement authorities.[146] The court directly considered the issue of the defendants' privacy interest in their test results, finding the law enforcement's use of these records acceptable, and noting:

> There is no objectively reasonable expectation of privacy in the test results. Clearly, defendants cannot claim ownership or possession of the results. Also, as stated in [*United States v.*] *Miller*, information revealed to a third party, even for a limited purpose, can properly be conveyed to the government even if the information was revealed in confidence. In these cases, blood was taken for a limited purpose, medical treatment. . . . [T]he information conveyed was not privileged. Under the *Miller* analysis, once the hospitals obtained the results for medical purposes, it would have been unreasonable for defendants to assume that the results would necessarily remain private. At the very least, various hospital employees become aware of the test results in the normal course of their work. Society places a risk on persons in their dealings with third parties that information conveyed to third parties will not remain private.[147]

Note that other cases lend support to the decision and reasoning in *Perlos*,[148] while clearly contrary opinions exist. For example, the court in *Commonwealth v. Riedel* found that, in a situation where law enforcement authorities searched an individual's medical records, the defendant did have "a reasonable expectation of privacy in his medical records," although the court found that the law enforcement search was lawful on the less controversial Fourth Amendment grounds of probable cause and exigent circumstances.[149]

---

[145] *See id.* at 312 ("These [blood] tests were made for medical treatment.").

[146] *Id.* at 323 (Levin, J., dissenting) (quoting MICH. COMP. LAWS § 257.625a(9) (1982)).

[147] *Id.* at 321 (footnotes omitted).

[148] *See, e.g.*, State v. Dyal, 478 A.2d 390, 395 (N.J. 1984) ("[T]he statutory patient-physician privilege does not prevent a blood test of one who is arrested on probable cause to believe he is intoxicated and who is taken by police in custody for diagnosis."); State v. Jenkins, 259 N.W.2d 109, 113 (Wis. 1977) ("[T]he defendant had no reasonable expectation of privacy concerning those [blood alcohol] test results.").

[149] 651 A.2d 135, 139 (Pa. 1994). Courts have also used similar reasoning to find that a hospital patient has a legitimate expectation of privacy in the blood taken for treatment itself, so that a police search inducing hospital personnel to supply some of this blood for alcohol content testing is invalid and illegal. *See* State v. Comeaux, 818 S.W.2d 46, 52 (Tex. Crim. App. 1991) (recognizing "society's regard for this expectation [of privacy], as evidenced by the Texas Medical Practice Act"), *overruled by* State v. Hardy, 963 S.W.2d 516 (Tex. Crim. App. 1997), *reh'g denied* (1998).

Cases in this area are not uniform in their treatment of the medical records privacy right. Marked differences exist in how courts assess the expectation of privacy, the interests of law enforcement, and the scope of any possible intrusion. As a result, although some support for a vigorous protection of medical records privacy may exist within this Fourth Amendment framework, this support seems uneven and questionable at best.

2. Problems with the *Miller* Reasoning in the Modern Health Information Context

Many of the cases centering on medical records privacy in the Fourth Amendment context use reasoning based on *United States v. Miller*.[150] This case dealt with the validity of subpoenas ordering production of all records of the bank accounts held by two of the defendant's banks.[151] The banks produced these records on microfilm, and at trial the defendant unsuccessfully sought suppression of these records, asserting that the subpoenas were defective.[152] The appeals court reversed,[153] but the Supreme Court found that there was "no intrusion into any area in which [the defendant] had a protected Fourth Amendment interest."[154]

The defendant appealed to the reasoning in *Katz v. United States*,[155] which expanded the Court's previously restrictive view that "'property interests control the right of the Government to search and seize,'"[156] and more importantly held that searches and seizures become unreasonable when the government's activities run afoul of the "privacy upon which . . . [individuals] justifiably rel[y]."[157] The Supreme Court in *Miller*, however, chose to focus on another issue raised in *Katz*, noting that the *Katz* Court "also stressed that '[w]hat a person knowingly exposes to the pub-

---

[150] 425 U.S. 435, 440 (1976) (holding that a bank depositor had no protectible Fourth Amendment interest in bank records, consisting of microfilms, checks, deposit slips and other records related to the depositor's accounts at two banks, despite the requirements of the Bank Secrecy Act and that the records were obtained by allegedly defective subpoenas).

[151] *See id.* at 436 (observing that the case arose when Miller "moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas . . . served upon two banks at which he had accounts").

[152] *See id.*

[153] *See* United States v. Miller, 500 F.2d 751, 758 (5th Cir. 1974) (holding that the trial court should not have admitted Miller's bank checks into evidence), *rev'd*, 425 U.S. 435 (1976).

[154] *Miller*, 425 U.S. at 440.

[155] 389 U.S. 347 (1967) (holding that the government's listening to and recording of a defendant's phone conversation from a public telephone booth using electronic surveillance equipment constituted an improper search and seizure without judicial sanction).

[156] *Id.* at 353 (quoting Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 304 (1967)).

[157] *Id.*

lic . . . is not a subject of Fourth Amendment protection.' . . . We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[158] The *Miller* Court went on to state that in reviewing the nature and content of bank records, it "perceive[d] no legitimate 'expectation of privacy' in their contents."[159] Indeed, the Court observed that

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[160]

Despite severe criticism of the result and reasoning in *Miller*,[161] and the harm it does to Fourth Amendment protections of privacy, the essence of the case remains good law.[162] More importantly, this case often serves as the philosophical foundation of court decisions which attack and undermine the expectation of privacy that individuals often assert with respect to law enforcement intrusion into personal health information.[163] Within both the medical records arena and the health care provider-patient relationship, as in the financial records context, a loss of privacy to unrestricted government

---

[158] 425 U.S. at 442 (quoting *Katz*, 389 U.S. at 351).

[159] *Id.*

[160] *Id.* at 443 (citations omitted). Note that in support of this statement, the Court relied on the line of "false-friend" cases concerning government informants' relaying of information received in supposed confidence. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the use of testimony of a government informer concerning conversations between the defendant and the informer did not violate the Fourth Amendment rights of the defendant).

[161] *See, e.g.*, Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. U. L. REV. 1, 22-29 (1983) (noting that "[r]eactions to the decision in *Miller* have been overwhelmingly negative" and challenging the finding in *Miller* that individuals assume the risk of disclosure of private information that they share with another).

[162] Although *Miller*'s holding as it relates to financial records has been limited by the Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. §§ 3401-3422 (1994), the case is still relevant for medical records privacy. In fact, commentators have argued that a similar result to that in *Miller* would occur if an analogous case involving medical information were to come before the Supreme Court, since *Miller* effectively governs the medical records context. *See, e.g.*, Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 290-91 (1984) ("As a practical matter, in the absence of a statute or a definitive court decision, the *Miller* decision is effectively being applied when medical records are subpoenaed." (citations omitted)).

[163] This is apparent in the *Perlos* decision discussed earlier. *See supra* notes 144-49 and accompanying text (discussing how the *Perlos* decision limits individuals' medical records privacy and expands law enforcement's use of such information).

access would cripple the privacy rights supposedly protected by the Fourth Amendment and other facets of the Constitution. If anything, it seems reasonable to assume that individuals might expect that a higher level of privacy will be afforded to their medical history. Moreover, both financial and medical records are subject to tremendous technological advancements that have spurred massive computerized record keeping.[164] Unfortunately, the post-*Miller* evolution of law enforcement's access to private medical information has left few real privacy protections in this area.[165]

The decision in *Katz* properly assessed the ownership and property facets of the Fourth Amendment protections by noting that such concepts cannot "serve as a talismanic solution to every Fourth Amendment problem";[166] yet, the *Miller* Court asserted that there can be no protected privacy interest where there is neither "ownership nor possession" of the thing sought to be kept private.[167] This logic fails to grasp the realities of changes in technology and societal structure, and has led to substantial erosion of privacy protections in the medical records-law enforcement area. Of course, one could consider some information collected by organizations in the course of dealings between patients and health care providers properly within the zone of information "a person knowingly exposes to the public,"[168] and therefore not subject to Fourth Amendment protection. On the other hand, information directly related to one's health—information gleaned from privileged communications between patient and doctor—should not be so easily classified as such.[169] Rather, the approach set forth in *Katz* seems more appropriate. In *Katz*, the court focused on two issues: (1) whether the defendant "exhibited an actual (subjective) expectation of privacy" in the records, and

---

[164] *See* Hellwege, *supra* note 29, at 22 (noting that the electronic storage and transmission of medical records creates an opportunity for people to inappropriately access the information).

[165] Multiple sources have noted this reality. *See, e.g.*, Thurman v. Texas, 861 S.W.2d 96, 101 (Tex. App. 1993, no writ) (concurring opinion) ("The unrestricted use of grand jury subpoenas to obtain medical records is a serious threat to privacy. There is almost no limit on what can be obtained without the knowledge or approval of any court, any grand jury, any supervisor in a prosecutor's office, or the person affected."); PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 377 (1977) (concluding after significant research that the subpoena was a mere "administrative tool" used by law enforcement to access individual medical records to circumvent Fourth Amendment restrictions).

[166] Katz v. United States, 389 U.S. 347, 351 n.9 (1967).

[167] 425 U.S. at 440.

[168] *Katz*, 389 U.S. at 351.

[169] Note that in *Miller*, law enforcement authorities proceeded under color of a subpoena, but the reasoning in *Miller* has been used to support information gathering using much more controversial means. *See, e.g.*, United States v. Payner, 447 U.S. 727, 732 (1980) (using *Miller* to uphold the validity of information acquired by IRS agents *via burglary*).

(2) if so, whether that expectation is one that "society is prepared to recognize as 'reasonable.'"[170]

In general, the social impetus behind HIPAA and the *HHS Report* help resolve these two questions. Although the first prong of the *Katz* analysis is dependent on the expectations of the individual defendant, the public sentiment that resulted in the Act's confidentiality protections and subsequent HHS recommendations indicates that, in most instances, individuals subjectively expect, and seek to insure, medical records privacy.[171] Such public opinion is a clearer response to the second inquiry in *Katz*: society appears willing to accept as reasonable general principles that strengthen medical record confidentiality laws. What remains at issue, then, is how these *Katz* questions would be answered in the specific context of law enforcement access to medical records. Thus, society must determine whether or under what circumstances law enforcement should be allowed access to this personal information. Currently, law enforcement officers can gain access to private medical information with relative ease, given the weak state of constitutional search-and-seizure protections for the privacy of medical information.[172] This reality, when coupled with the impending likelihood of federal legislation on this issue in the near future, creates an ideal opportunity to reconsider our stance on law enforcement's ability to access this personal information.

C. *Federal Laws*

Congress has enacted federal legislation that impacts individuals' health information privacy and law enforcement's access to such records. The two major statutes governing the issue are the Privacy Act and the Freedom of Information Act. In addition, various other laws permit medical records review by various federal agencies.

1. The Privacy Act

The Privacy Act of 1974[173] ("the Privacy Act") ensures that federal agencies utilize fair information practices with regard to the collection, management, use, and dissemination of any record within a system of rec-

---

[170] 389 U.S. at 361 (Harlan, J., concurring).

[171] *See supra* notes 10-12 and accompanying text (discussing public perception of medical records confidentiality).

[172] *See supra* note 165 and accompanying text (noting that few protections exist against law enforcement access).

[173] 5 U.S.C. § 552a (1994).

ords.[174] Subject to exemptions, the Privacy Act prohibits disclosure of information to another person or agency without prior written consent by the individual to whom the data relates.[175] The Privacy Act allows an individual to review, copy, and correct mistakes in records pertaining to that individual.[176] The law also prescribes limits on the collection and maintenance of information by agencies, allowing agencies only to keep information that is necessary for the purpose of the agency required to be accomplished by federal statute.[177]

Federally run hospitals and health care providers and research organizations which receive federal funding must maintain patient records that comply with the Privacy Act.[178] It is not difficult, however, for agencies to avoid the Privacy Act's central purpose of privacy protection. Federal organizations may disclose and use information for a so-called "routine use," so that health information can be used for any "purpose which is compatible with the purpose for which [the health data] was collected."[179] This "routine use" exception would allow, for instance, HHS to use Medicare or Medicaid databases as a monitoring and law enforcement tool to protect against fraud and abuse, even if the original purpose of the files was to promote public and individual health.[180]

---

[174] The term "record" is defined in the Privacy Act as follows:

> [T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number[] [or] symbol . . . assigned to the individual, such as a finger or voice print or photograph . . . .

Id. § 552a(a)(4).

"System of records," in turn, is defined at 5 U.S.C. § 552a(a)(5) ("[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, [or] symbol . . . assigned to the individual . . . ."). Note that individuals' confidential health information currently collected by myriad federal agencies typically fits within this definitional framework.

[175] *See id.* § 552a(b) ("Conditions of disclosure").

[176] *See id.* § 552a(d)(1)-(4) ("Access to records").

[177] *See id.* § 552a(e) ("Agency requirements").

[178] *See, e.g.*, OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION, OTA-TCT-576, at 42 (1993) (stating that the Federal Privacy Act is applicable at hospitals that maintain registers of cancer patients pursuant to a federal contract).

[179] 5 U.S.C. § 552a(a)(7).

[180] Indeed, one explanation for HHS's reluctance to draft strong recommendations which would limit law enforcement access to private medical information is that HHS also fulfills a significant law enforcement role itself with respect to Medicare and Medicaid fraud and does not want to limit its own abilities in this area. Interview with Professor John Merz, Center for Bioethics, University of Pennsylvania, in Phila., Pa. (Oct. 7, 1997).

Finally, the Privacy Act provides substantial exceptions for law enforcement authorities. These exceptions effectively minimize any privacy protection that the law might offer to individuals against improper law enforcement intrusion into their medical records. For example, any law enforcement agency of any governmental unit can acquire personal records (including medical information) without notice or consent, merely if the agency claims that such records will be used for "law enforcement activity."[181] A host of other law enforcement-related exceptions essentially swallow the protections afforded by the Privacy Act with respect to law enforcement's access to medical information.[182]

2. The Freedom of Information Act

The intent of the Freedom of Information Act[183] ("FOIA") is to protect the rights of citizens to obtain access to government information held by federal agencies, and Congress did not intend for the Privacy Act to interfere with these rights. However, FOIA contains a series of exemptions to its general provisions that permits agencies to withhold information and thus protect confidential records from improper disclosure. For example, HHS typically uses Exemption Three[184] to protect health data,[185] and the Centers for Disease Control ("CDC") has relied in the past on Exemption Four for similar purposes.[186] Exemption Six protects "medical files" if their disclosure "would constitute a clearly unwarranted invasion of personal privacy."[187] The Supreme Court has determined that when a party seeks FOIA disclosure concerning individually identifiable records, a court must review the potential disclosure by employing a balancing test that weighs the individual's privacy right against the public's interest in the information in question.[188]

---

[181] 5 U.S.C. § 552a(b)(7).

[182] For an excellent overview of how these exceptions interrelate, see GUIDEBOOK TO THE FREEDOM OF INFORMATION AND PRIVACY ACTS 55-57 (Robert F. Bouchard & Justin D. Franklin eds., 1980).

[183] 5 U.S.C. § 552.

[184] *See id.* § 552(b)(3) (exempting data specifically excluded from FOIA disclosure requirements by statute).

[185] *See, e.g.*, 42 U.S.C. § 247c(e)(5) (1994) (restricting disclosure of sexually-transmitted disease records by HHS).

[186] *See* 5 U.S.C. § 552(b)(4) (exempting "privileged or confidential" data). For an example of the CDC's application of this exception, see *Washington Post Co. v. United States Department of Health & Human Services*, 690 F.2d 252, 258 (D.C. Cir. 1982) (discussing the evidentiary privilege of Exemption Four).

[187] 5 U.S.C. § 552(b)(6).

[188] *See* Department of the Air Force v. Rose, 425 U.S. 352, 370-75 (1976) (discussing the balancing test employed in an Exemption Six inquiry).

Although FOIA might provide some medical records protection against law enforcement intrusion, its exemptions are subject to significant limitations. Generally, agencies have the discretion, not the duty, to withhold disclosure if one of the exemptions applies, and an "agency decision is reversible only if arbitrary or capricious."[189] Also, reliance on a balancing test and judicial review in this situation may not adequately protect individual privacy rights in the medical record-law enforcement arena.[190]

3. Other Laws

Statutory initiatives over the past several years have expanded the authority of federal agencies to obtain private medical records in a host of instances, often for monitoring and law enforcement purposes. As Robert Gellman notes, "The growth of government involvement in health matters has resulted in an expansion of the power of government agencies to compel the production of records."[191] For instance, the Food and Drug Administration enjoys a legal right to the information and records collected in connection with new drug trials,[192] and HHS officials enjoy subpoena power for both the administration of Medicare[193] and the detection of fraud and abuse.[194] These are only a few of the numerous examples of this type of statutorily based power.

D. *State-Level Legal Frameworks*

Although legal developments in state courts and legislatures have produced some protection for individuals' medical histories, these sources of law are characterized more by their diversity and conflicting standards than by the quality of protection they afford. In particular, the cases and state laws offer little additional support for medical records protection from law

---

[189] GUIDEBOOK TO THE FREEDOM OF INFORMATION AND PRIVACY ACTS, *supra* note 182, at 62 (footnote omitted).

[190] As support for this assertion, Gostin cites the decision in *United States v. Providence Hospital*, 507 F. Supp. 519 (E.D. Mich. 1981), noting that the holding of this case validated an IRS subpoena of hospital substance abuse records because this law enforcement interest outweighed the individual privacy interests involved. *See* Gostin, *supra* note 8, at 503 & n.251.

[191] Gellman, *supra* note 162, at 287.

[192] *See* 21 U.S.C. § 355(k) (1994) (regulating access to records pertaining to drug applications).

[193] *See* 42 U.S.C. § 1395ii (1994) (giving the HHS secretary the subpoena power in Medicare investigations by incorporating 42 U.S.C. § 405(d) into the Medicare laws).

[194] *See* Inspector General Act of 1978, §§ 2, 6(a)(4), Pub. L. No. 95-452, 92 Stat. 1101, *reprinted in* 5 U.S.C. app. 3, at 1381, 1386 (1994) (providing for an "Inspector General" of HHS, and giving subpoena power to this office to "prevent and detect fraud and abuse").

enforcement intrusion. This Subpart reviews tort- and contract-based cases and considers relevant medical information privacy laws.

1. Cases

In general, when a patient believes that a health care provider has improperly divulged her private medical information, she may have as many as five causes of action: breach of fiduciary relationship, negligence, breach of implied term of contract, defamation, and invasion of privacy.[195] Professional negligence and breach of fiduciary duty claims are appropriate when doctors disclose confidential information.[196] The essence of these two approaches is that the professional owes the patient a duty of confidentiality as part of the proper care that accompanies a doctor-patient relationship.[197]

Breach of contract claims rest on the notion that there exists an implied contract made by the health care provider to maintain the confidentiality of personal matters revealed during treatment.[198] The rationale for the last two theories, defamation and invasion of privacy, is that medical information is "highly personal" and that patients have a right of protection against "mass dissemination of information concerning private, personal matters."[199] Defamation and invasion of privacy typically entail a balancing of the patient's privacy rights with competing interests.[200] As previously noted,

---

[195] *See* Pamela K. Sutherland & Gina Yarbrough, *High-Tech Gossip: Physician-Patient Confidentiality and Computerized Managed Care*, TRIAL, Nov. 1996, at 59 (listing the five possible causes of action); *see also* Gostin, *supra* note 8, at 508-09 (listing four of the five theories).

[196] Commentators often combine negligence and breach of fiduciary duty claims into a single category, breach of confidentiality, when describing claims of wrongful disclosure of confidential information. "The gravamen of both negligence and breach of fiduciary duty claims is that the professional owes [the] patient a duty of confidentiality within the bundle of duties of proper care that accompanies a professional-patient relationship." Sutherland & Yarbrough, *supra* note 195, at 60. Similarly, William Roach notes that when a "health care provider . . . improperly discloses medical records information," the patient may sue on the theory of "breach of confidentiality." WILLIAM H. ROACH, JR. & THE ASPEN HEALTH LAW AND COMPLIANCE CTR., MEDICAL RECORDS AND THE LAW 274 (3d ed. 1998).

[197] *See, e.g.*, Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801-02 (N.D. Ohio 1965) (validating the fiduciary duty theory); Alexander v. Knight, 177 A.2d 142, 146 (Pa. Super. Ct. 1962) (finding that there exists a "duty of total care" that includes a "duty to refuse affirmative assistance to the patient's antagonist in litigation").

[198] *See, e.g., Hammonds*, 243 F. Supp. at 801 (stating that the contract between doctor and patient includes, "as an implied condition," an understanding that "confidential information gained through the relationship will not be released without the patient's permission").

[199] ROACH & THE ASPEN HEALTH LAW AND COMPLIANCE CTR., *supra* note 196, at 266.

[200] *See id.* at 260-74 (noting that in defamation cases, a conditional privilege is available to the defendant if she can prove that the information published affects a "sufficiently important interest" of the publisher, and that in invasion of privacy cases, courts compare the right to "protect against mass dissemination" with "matter[s] of legitimate public concern").

courts tend to be deferential when weighing governmental interests in obtaining and using personal medical records;[201] this is true in these specific legal contexts as well.[202]

Although these legal options are applicable to the disclosure of personal medical information to law enforcement authorities, a number of practical and legal limitations exist that undercut the efficacy of these protections. Practically, such actions arise after an improper disclosure. This minimizes the ability of the potential remedy to put the plaintiff in the position of maintaining his privacy—it is simply too late, since the disclosure has occurred. Also, the proliferation of computerized record keeping and database management creates medical information sources—and potential abuse of these sources—that are completely unknown to the patient.

Legally, exceptions to the general duty of confidentiality render these common law actions useless. Gostin observes that "[t]hese claims are weakened to the extent that courts recognize justifications [for disclosure] other than consent."[203] Gostin goes on to identify a number of such exceptions that could apply to the law enforcement question and concludes that although "common law protection of confidentiality probably provides the most consistent safeguards, significant gaps exist in legal duties."[204] Indeed, some of the most well-defined exceptions are those statutorily based exclusions that center on law enforcement's ability to obtain and use confidential medical records.[205] Finally, some legal scholars view with antipathy the legal concept upon which these actions are founded—the privilege of

---

[201] *See supra* Part II.A.2 (discussing cases that seem to restrict protections for medical records privacy because of court deference to governmental interests).

[202] *See, e.g.*, Bratt v. IBM, 467 N.E.2d 126, 135 (Mass. 1984) (discussing the balancing test to be employed in the context of private business communications); ROACH & THE ASPEN HEALTH LAW AND COMPLIANCE CTR., *supra* note 196, at 262-64 (discussing the strong privilege protecting publications made in "legislative, judicial, and administrative proceedings" and noting that a qualified privilege exists for other public acts).

[203] Gostin, *supra* note 8, at 509.

[204] *Id.* at 510.

[205] The subpoena power that many federal agencies enjoy is an example of a statute-based exclusion. *See supra* Part II.C.3 (discussing statutory initiatives giving federal agencies the power to obtain private medical records). Also, a number of more specific exceptions exist in state statutes, including physician reporting requirements for gunshot wounds, child abuse, and communicable diseases. *See, e.g.*, Gellman, *supra* note 162, at 274 & n.78 ("Every state requires health care providers to report selected identifiable patient information to state agencies."). The *Perlos* decision discussed in Part II.B.1 dealt with a Michigan statute requiring physicians to take blood from auto accident victims, analyze it for alcohol content, and submit results to the police. *See* People v. Perlos, 462 N.W.2d 310 (Mich. 1990); *supra* notes 144-47 and accompanying text.

confidentiality between doctor and patient.[206] As a result, these common law-based approaches tend to offer few restrictions on law enforcement's access to and use of medical records.

2. State Statutes

There is tremendous variation in the level of protection afforded individuals by state laws governing medical records privacy. When the law is comprehensive and well-considered, it can provide substantial protections. Often, more complete legislative efforts prohibit providers from disclosing identifiable information excepting only the situation where patients provide consent for such disclosures, or under a relatively small number of clearly defined exceptions in the law.[207]

More typically, state "practice acts" that license doctors and other health care providers or state laws that regulate hospitals frequently contain language restricting disclosures of health information.[208] Unfortunately, the ambiguity inherent in these legislative efforts often leaves the patient with little concrete protection from law enforcement intrusions and the health care provider with little guidance on what circumstances warrant protection of a patient's health information. Indeed, Professor Gellman argues that this lack of guidance is common, leaving providers with a morass of ethical and legal problems when faced with a demand by law enforcement for private medical information.[209] In addition, since many such legislative initiatives

---

[206] *See, e.g.*, JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §§ 2285, 2380a (McNaughton rev. ed. 1961) (disputing, among other aspects of the privilege, whether physician-patient communications should be confidential).

[207] For examples of state laws that provide substantial and comprehensive protections of medical privacy, see CAL. CIV. CODE §§ 56-56.37 (West 1982 & Supp. 1995) and Confidentiality of Health Care Information Act, R.I. GEN. LAWS § 5-37.3-1 (1995). Commentators observe that only a small number of state medical records confidentiality laws tend to fit this description. *See, e.g.*, Gellman, *supra* note 162, at 278-79 ("A 1979 review of state laws concerning health records confidentiality by the National Commission on Confidentiality of Health Records (NCCHR) concluded that the great majority of states had not completed comprehensive statutes to regulate the record keeping practices of health care providers."); Gilbert, *supra* note 32, at 93-94 ("[A] wide range of laws that attempt to preserve the confidentiality of health information currently exist. Unfortunately, since there is no concerted effort, there is no uniformity in the protection, or lack thereof, provided by these statutes."); *see also* HHS REPORT, *supra* note 18, pt. I.B (describing the inadequacies of current state regulation).

[208] *See, e.g.*, Berry v. Moench, 331 P.2d 814, 817 (Utah 1958) (discussing a violation of Utah's practice act regarding physician-patient confidentiality).

[209] *See generally* Gellman, *supra* note 162, at 255-94 (arguing that existing legal and ethical guidance in general is inadequate to aid physicians in addressing confidentiality issues raised when patient information is demanded or requested from them). In particular, Professor Gellman discusses the uncertainties that characterize the physician's decision to provide

rest ideologically on the physician-patient privilege, the drastic narrowing of this patient right and concomitant expansion of exceptions to this rule[210] practically eviscerate the philosophical foundations upon which lie privacy protections in the law enforcement-medical records area. The most important aspect of this narrowing is that the privilege rarely applies outside of the strict, two-person doctor-patient relationship.[211] Given the realities of modern medical care delivery, where multiple teams of health care providers work with a single patient, and the expansion of authorized users of personal health care information, the privilege seems poorly equipped to protect individuals' privacy interests from law enforcement intrusion.

E. *Concluding Observations About the Legal Landscape*

From this overview, it becomes clear that the existing legal protections afforded to individuals seeking to assert a privacy interest in their health records and prevent law enforcement intrusion are more disparate than standardized, more ambiguous than defined, more conflicted than robust, and more incomplete than comprehensive. Importantly, the overwhelming majority of this body of law rests on principles and notions that may fail to capture the imperatives laid bare by the rapid computerization and technological change in health care delivery. Given this evaluation, it seems curious and unfortunate that HHS missed the chance to devise substantive recommendations regarding law enforcement's use of private health information. Part III of this Comment critiques the HHS proposal and existing laws generally, in an effort to extricate some potential concerns that Congress might consider if and when it addresses the issue of health information confidentiality.

---

information to law enforcement. *See id.* at 281-87 (discussing discretionary disclosures of a physician).

[210] Professor Gellman provides an excellent overview of these developments:

> First, the privilege is a testimonial privilege. It only applies when the physician is testifying in court or in related proceedings. This represents only a small fraction of the disclosure demands that may confront a physician .... Second, the privilege is much narrower than it seems. Statutory exemptions and judicial restrictions have so limited the privilege in many states that the protections are only rarely available .... Third, the privilege does not exist in all states.

Id. at 272-73.

[211] *See* Gostin, *supra* note 8, at 507 ("In many states, the privilege is limited to physicians and therapists and does not extend to the great majority of health care professionals." (footnote omitted)).

III. ARGUMENTS FOR STRENGTHENING THE LAW ENFORCEMENT EXCEPTION OF THE HHS PROPOSAL

If the dramatic changes in technology and health care delivery demand a reevaluation and standardization of current privacy protections in this area, and present legal protections against law enforcement intrusion can plausibly be deemed inadequate or at least unclear, then it seems reasonable to criticize the *HHS Report* for failing to address these realities in its proposed law enforcement exception. In constructing this critique, one can make a number of arguments. Briefly, the law enforcement exception's perceived shortcomings can be grouped into five areas: (1) it fails to acknowledge important moral and social arguments for a more limited exception; (2) it does not adequately address concerns that technological changes render current Fourth Amendment law inadequate; (3) it omits full consideration of other constitutional and legal arguments; (4) its call for federal legislation frustrates standardization imperatives in the law enforcement sphere; and (5) its proposed penalty-based approach fails, at least in part, in the law enforcement context.

A. *Moral and Social Arguments for a More Limited Exception*

Numerous commentators have offered thoughtful and compelling moral justifications for establishing privacy rules and laws in general.[212] These arguments tend to support the assertion that lawmakers should establish a strong, consistent set of rules governing law enforcement's use of private medical records. One major moral rationale for establishing privacy rules is that respect for autonomy is entwined with respect for privacy. As Gostin states, "To respect the privacy of others is to respect their autonomous wishes not to be accessed in some respect—not to be observed or have information about themselves made available to others."[213] Gostin goes on to note that respecting privacy promotes "a sense of self and of personhood," which in turn allows individuals to "develop the capacity to be self-governing."[214] These are important moral goals that can have utilitarian benefits as well.[215]

---

[212] *See, e.g.*, Gellman, *supra* note 162, at 266-81 (detailing the different sources, such as the ethical principles of the medical profession and state and federal law, from which physicians can derive privacy rules having to do with disclosure of patient information); Gostin, *supra* note 8, at 513-16 (describing several "ethical justifications for informational privacy").

[213] Gostin, *supra* note 8, at 513-14.

[214] *Id.* at 514.

[215] For instance, one might hope that the self-governing individual will not require law enforcement surveillance or investigation to the same extent as another individual lacking such internal control.

Additionally, the assertion that privacy protection from law enforcement intrusion into medical records promotes the development "of intimate human relationships—relationships of trust" supports such protection.[216] Gostin also acknowledges the benefits of this moral imperative, noting that an "expectation of privacy allows individuals to confide freely in their physicians."[217] The law should recognize harm to an individual's moral rights as a harm in itself without requiring a showing of any consequential practical harm.[218] The notion that this moral benefit also has utilitarian social ramifications—improved confidence in the provider-patient relationship—should result in improved communication between patient and doctor, and hence improved care. Indeed, although some scholars have recognized certain aspects of this benefit,[219] one should analyze the multitude of facets to this general social benefit with particularity.

First, improving care could benefit not only the individual, but also society. As these beneficial individual experiences accumulate at a societal level, they will reduce the costs of Medicare and other government-funded health care programs which later assume responsibility for financing such interventions. Also, improved communications between doctor and patient should improve the accuracy of data that supports public health research, and hence public health. Finally, more open communication could ostensibly lower the individual's cost of care, as honest, open communication reduces the need for expensive diagnostic procedures by narrowing the scope of the physician's inquiry.

Promulgating a standard of privacy that is markedly unrestrictive for law enforcement's use of medical records would severely undermine these moral and resulting social benefits. Such a failure in privacy protection might undercut any achievements sought by the remainder of the *HHS Report*. Undoubtedly, the moral demands for privacy are valid, and the societal benefits which flow from these moral imperatives are substantial. Importantly, lawmakers can only protect these moral and social benefits in the

---

[216] Gostin, *supra* note 8, at 514.

[217] *Id.*

[218] *See, e.g.*, Doe v. Southeastern Pa. Transp. Auth. (SEPTA), 72 F.3d 1133, 1147 (3d Cir. 1995) (Lewis, J., concurring and dissenting) (asserting that the lack of direct harm to an individual should not figure in the analysis of determining whether an improper intrusion into that individual's medical records gives rise to liability).

[219] Gellman, for example, notes that the "'assurance of confidentiality encourages patients to be candid with their physicians, and candor is essential to effective diagnosis and medical management of the patient's ailments.'" Gellman, *supra* note 162, at 257 (quoting *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before the Gov't Info. and Individual Rights Subcomm. of the House Comm. on Gov't Operations*, 96th Cong., 1st Sess. 1129 (1979) (statement of James H. Sammons, M.D., Executive Vice President, American Medical Association)).

rapidly changing context of technology and health care delivery if they reassess how best to protect these benefits in light of the larger societal changes.[220] The *HHS Report* completely fails to acknowledge these moral and social reasons for review of the law enforcement exception, and therefore puts at risk both the moral imperatives and their concomitant social benefits. This seems especially unsettling, given the government's increased presence as a participant in the health care delivery system, and its resultant increased role as police officer in the health care arena.[221]

B. *Realities of Technological Change: The General Need for Reevaluation and the Fourth Amendment Problem*

As this Comment demonstrates, the technological advances in health care delivery and health information usage have been so rapid and profound that many paradigms related to health care have been rendered obsolete.[222] There is no doubt that this obsolescence is also true of the legal framework for medical records privacy protection. Indeed, both HIPAA and the *HHS Report* are responses to these transformations.[223]

Plainly, law enforcement's use of private medical records is subject to these same realities of change. However, the *HHS Report* fails to consider how these changes have altered the balance between law enforcement's access to medical histories and individuals' privacy interests—this is a crucial flaw in its recommendations concerning the law enforcement exception. Consider for example a scenario suggested by Senator Frist during Secretary Shalala's recommendations testimony: during a fraud and abuse inspection of Medicare records, HHS investigators discover information that may indicate criminal activity, and pursue this possible lead.[224] The discovered information is highly confidential and would be damaging to the individual's

---

[220] Judith DeCew briefly mentions this need for reevaluation of legal constructs to protect moral imperatives in light of technological change, noting that "technological advances without restriction often erase one's ability to maintain privacy and control information about oneself." DECEW, *supra* note 114, at 162.

[221] *See, e.g.*, Gellman, *supra* note 162, at 260-61 ("With the implementation of Medicare and Medicaid in 1966, the share of the nation's health bill paid by government increased significantly.... These programs, which include ... fraud, abuse, and waste investigations, frequently require access to identifiable patient information to carry out their functions." (footnotes omitted)).

[222] *See* discussion *supra* Part I.A (reviewing the changes in information technology and medical research, and the concurrent transformation of health care delivery).

[223] *See* discussion *supra* Parts I.B.1-2 (describing the influence of changes in health information technology, health care delivery, and medical records usage on the passage of HIPAA and the *HHS Report*).

[224] *See Hearings Statement*, *supra* note 81, at 9.

privacy interests if exposed.[225] At this level of description, it seems that the technology of modern database searching has aided law enforcement in identifying and pursuing crime, with little practical harm to the privacy rights of law-abiding citizens.

Yet, further examination reveals a murkier picture. Although sophisticated data mining techniques make collateral collection of information possible, such technological advances do not provide appropriate decision-making guidance to law enforcement, and can in fact lead to harmful results. Suppose further that law enforcement acted on the results of its data mining, yet found (only after revealing the confidential information and thus harming the individual's privacy interests) that the information was erroneous, incomplete, or led police to the wrong conclusion.[226]

It is this fundamental change in how searches are conducted, driven by technological changes and the computerization of private medical records, that raises concerns. These changes relate not only to the potentially expanding scope of law enforcement intrusions, but also to the changes in technology that render current legal limitations in this area ineffective. For example, the Fourth Amendment case underlying much of law enforcement's ability to search medical records, *United States v. Miller*, rests on the notion that there can be no protected Fourth Amendment interest where there is neither ownership nor possession of the "property" in question.[227] Such a formulation of this interest clearly would exclude medical information stored in modern client-server or database architectures. As a consequence, the mixture of this outmoded legal reasoning and modern developments in computerization of medical records leads to a sharp and violent curtailment of the privacy protections that individuals should and rightly do expect in this area. To leave such results in place, as the HHS recommen-

---

[225] *See id.*

[226] There is precedent for this unfortunate result. In an apt analogy, Dr. Margo Goldmans, a Boston psychiatrist, described how marketers performed data mining on medical records, and based on the results, assumed that a patient of hers was receiving treatment for impotency. The resulting flow of junk mail caused considerable embarrassment for the individual, and undermined his confidence in the therapist-patient confidentiality. *See All Things Considered: Data Mining Regulations* (NPR radio broadcast, Aug. 26, 1997).

Note the similarity between this scenario and one where police, allowed to cast an unfettered net over confidential medical records, could draw conclusions and make arrests that not only were in error, but also led to considerable harm, and undermined patients' confidence in the doctor-patient relationship. The *HHS Report* specifically addresses the scenario Dr. Goldmans describes, yet fails to consider the plausible law enforcement analogy, allowing it to remain a distinct possibility.

[227] 425 U.S. 435, 440 (1976) (finding that the Fourth Amendment does not protect individuals' interests in records maintained by banks pursuant to the Bank Secrecy Act, because the individuals could assert "neither ownership nor possession" over the banks' business records).

dation on the law enforcement exception does, seems incongruous with the balance of the *Report*'s appreciation for the legal impact of technological change, and counter to citizens' expectations of privacy in a modern, technological society.

C. *Other Constitutional and Legal Arguments for a More Limited Exception*

Changes in technology and health information management should drive a critical reevaluation of laws that potentially govern law enforcement's usage of private health records. The privacy cases, both those at the Supreme Court level seeking to identify a constitutional right to privacy,[228] and the tort- and contract-based cases at the state level,[229] often employ a balancing of interests framework. This allows for a certain flexibility in judicial decision making, and would thus seem to provide some adaptability for this legal approach as technology transforms health care and the usage of private health information. Indeed, the first major privacy case at the Supreme Court level to focus on governmental intrusion into individuals' health records privacy, *Whalen v. Roe*,[230] identified this very issue. Although in his concurrence Justice Brennan agreed with the results of the balancing test upholding New York State's right to collect confidential prescription records for addictive drugs, he was concerned about the changing nature of technology and its effect on the government's ability to intrude into personal medical records. "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information contained in the data, such as [confidential medical information], and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[231]

There is no doubt that later cases exhibit great deference to asserted governmental interests. Unfortunately, the courts in these cases have not heeded Brennan's warning that technological advances should drive a reevaluation of the relative weights of these interests,[232] despite the potential

---

[228] *See supra* Part II.A.1 (reviewing the line of Supreme Court cases developing a non-Fourth Amendment, constitutionally-based right to privacy).

[229] *See supra* Part II.D.1 (briefly reviewing common law causes of action available to an individual seeking to redress improper access or use of the individual's private medical records).

[230] 429 U.S. 589, 600 (1977) (holding that a statute authorizing a state to record the name, address, and age of patients who receive prescriptions for certain dangerous, legitimate drugs did not violate any constitutional rights to privacy).

[231] *Id.* at 607 (Brennan, J., concurring).

[232] *See supra* Part II.A.2 (analyzing cases following *Whalen* that demonstrate increased deference to government intrusions into medical records privacy).

harm such changes in health information management and usage can cause.[233] Courts readily embrace governmental justifications for privacy intrusions, while they receive arguments decrying the more troubling aspects of the new computerization and use of private health data less warmly. Assuming that this imbalance will only be further exacerbated as technology and the use of health records advance, the *HHS Report* should have at least acknowledged this as a potential problem in the area of law enforcement's use of medical information, and as a justification for a more serious review of current law enforcement uses of private medical data. Moreover, legal commentators have put forth convincing arguments that should shift courts' current weighing of the opposing interests,[234] and the HIPAA mandate offered an excellent opportunity to at least consider these arguments. Nevertheless, HHS let this opportunity slip away, failing to raise this important issue in its recommendations for legislation.

Instead, HHS recommended that the current state of this balancing approach be retained in the law enforcement context, despite its inherent uncertain and unfavorable attitude toward privacy. Removing this uncertainty would strengthen patient confidence in communication with their health care providers, and this would help further social benefits already described. On the other hand, uncertainty chills communication and lessens the efficacy of health care delivery. Moreover, the importance of this constitutional right demands that it be accorded a certain level of clarity; the intangible, moral benefits of the right are made real by clear rules describing law enforcement's ability to obtain and use private health records.

---

[233] *See supra* note 136 and accompanying text (discussing the medical records disclosure at issue in the *Doe* case).

[234] Many have argued that since the government is the primary collector and user of private information, individuals should not have to rely on that same government's discretion in protecting their privacy rights. Instead, commentators believe that an effective constitutional shield is required to prevent improper government (and thus law enforcement) intrusion into private information. *See, e.g.*, Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 133-35 (1991) (describing the conflict between the "government as 'collector' and . . . as 'protector,'" and arguing for a constitutional right to informational privacy).

Furthermore, another scholar has suggested that when performing the balancing typical in law enforcement privacy intrusion cases, courts fail to consider the significant value to the general public of the individual's privacy protection. In this sense, the balancing does not consider the governmental interest in preserving privacy when constructing its own policies and procedures. *See* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 147 (1991) (noting that government "[o]fficials who take seriously the [privacy] rights enunciated by the courts . . . [should] take into account the citizen's interests in privacy when constructing government operating procedures").

D. *The Need for Federal-Level Law in the Law Enforcement Context*

Although the *HHS Report* recommends that Congress enact federal legislation, adoption of the HHS position on the law enforcement exception would do no more than codify the current morass of incomplete and often conflicting rules covering this aspect of medical information privacy.[235] HHS recommends federal legislation primarily to rectify the inconsistencies concerning other facets of health information privacy,[236] but ironically, codification of this unwieldy body of law would only entrench the ambiguity currently characterizing law enforcement's use of medical records. As with other areas of the HHS proposal, federal legislation should standardize the law enforcement exception, not ossify confusion and incompleteness. More general arguments for federal-level standardization of health information privacy echo this concern and also support the implementation of clear federal standards governing law enforcement usage of such information.[237]

Moreover, the few examples of state-level standardization of the law enforcement exemption have met with generally favorable opinions.[238] Federal level uniformity would not result in absolute privacy rights, but instead would allow patients, physicians, and law enforcement officers to make correct decisions more easily by knowing in advance what rules guide their actions. In contrast, these parties are often ignorant of, or torn by, potentially competing claims and interests. For example, doctors commonly face contradictory interests and imperatives, such as a patient's confidentiality and a third party's safety from harm by that patient.[239] Undoubtedly

---

[235] Recall that the *HHS Report* proposes merely to recognize existing state laws regarding standards of law enforcement access to confidential medical information. *See* HHS REPORT, *supra* note 18, pt. II.D.10 (acknowledging that the proposed rules for law enforcement are "an exception to the basic principle of the protections" espoused by the *HHS Report*, and asserting that any legislation should merely "maintain current practices" of the existing patchwork of laws).

[236] *See id.* pt. I.B (recognizing and approving a need for federal legislation generally).

[237] *See, e.g.*, Gostin, *supra* note 8, at 516-17 (reviewing the general arguments for federal preemption in the medical records privacy area).

A related and significant practical reason for standardization in this context is that often the large number of authorized health information users are too confused by the variations among the conflicting legal standards to attempt to comply with them when faced with a demand for information from law enforcement. Many users assume that law enforcement authorities are certain of their rights regarding access to confidential medical information and therefore rarely challenge such requests. Interview with Mark Davidson, *supra* note 34.

[238] *See, e.g.*, Gellman, *supra* note 162, at 278-79 (assessing Rhode Island's clearly defined exceptions to medical record confidentiality, including its treatment of the law enforcement exception).

[239] *See, e.g.*, Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 343-46 (1976) (finding that third parties have an actionable interest in disclosure by physicians to prevent harm by physicians' patients).

this is a close question that cannot be reduced to a precise legislative rule, but certainly a federal law in this area could clarify the relevant issues for physicians, thereby increasing the likelihood of correct decisions and outcomes.

E. *Concerns Over the Proposed Legislation's Penalty-Based Approach in the Law Enforcement Sphere*

The *HHS Report* makes clear that it recommends no substantive changes to current law governing police usage of medical records, but it does suggest a somewhat novel approach to administering the current restrictions on law enforcement. Instead of reforming this area of the law, the *HHS Report* recommends that law enforcement personnel be subject to the penalties proposed in the *Report*.[240] Secretary Shalala explains this approach as such: "What we are not doing is changing current access laws by law enforcement. What we are doing is adding very severe penalties if they misuse that access."[241] Such an approach, however, begs the question of whether the "current access laws" are clear enough such that "severe penalties" can be meted out in a judicially consistent and effective manner. If the laws are too weak, too conflicted, and too incomplete, then how will judges decide when to impose penalties for their transgression? This is a looming question in light of the current state of access laws and the penalties-based solution in the proposed legislation. If the laws are not clear, then the penalties lose their efficacy and are unlikely to deter improper law enforcement conduct.

More importantly, privacy interests in medical records are protected only by preventing disclosure, not by punishing it. Rather, a clearly defined and strictly tailored set of law enforcement exceptions would go much further toward promoting the moral, social, and constitutional imperatives embodied in privacy interests than would a set of penalties for transgressions of poorly defined guidelines. A penalties-based approach seems especially inappropriate in light of the confused and lax current state of the law in this area.

---

[240] *See* HHS REPORT, *supra* note 18, pt. II.D.10 (asserting that "[w]e are not recommending any changes to existing legal constraints that govern access to or use of patient information by law enforcement agencies" and that "our recommendations would make obtaining health information under false pretenses be a Federal felony").

[241] *Hearings Statement*, *supra* note 81, at 14.

IV. TOWARD AN IMPROVED LAW ENFORCEMENT EXCEPTION: RECOMMENDATIONS

Given the criticisms of the proposed HHS recommendations for federal legislation, some proposals for possible improvement are warranted. The suggestions that follow are grouped into four general categories: (1) enacting a standardized federal law governing law enforcement's access to medical records; (2) establishing more stringent standards within the interest-balancing context and altering the state of Fourth Amendment law in this area; (3) broadening and strengthening physician-patient confidentiality; and (4) accommodating technological changes in medical information management and usage. The following recommendations hopefully would provide some insight into how changes in information management and use in the medical arena intersect with potential legal paradigms governing law enforcement's use of this information. More importantly, however, these suggestions are meant to embrace the benefits of technology for both medicine and law enforcement, as well as to introduce solutions that accommodate the important privacy interests implicated by the new, technologically-driven world.

A. *Enact a Standardized Federal Law*

At this point, the need for, and benefits of, standardized federal rules governing law enforcement use of private medical information should be clear.[242] Indeed, the advocacy of a federal law governing medical records privacy in general is not novel.[243] There is, however, an additional argument for enacting specific federal laws governing this area of privacy. This argument is especially timely given the structure and nature of both HIPAA and the *HHS Report*. At present, should Congress fail to act by August 1999, HIPAA mandates that HHS must write federal regulations to take effect no later than six months after that time.[244] Although this provision guarantees that some regulations will be in place by the end of 1999, such an approach would not offer the strongest and clearest set of law enforcement access rules or the best possible set of medical records privacy laws.

---

[242] *See supra* Part III.D (describing arguments in support of a standard federal law to clarify law enforcement's ability to access and use confidential medical records).

[243] *See, e.g.*, Gostin, *supra* note 8, at 516-17 (stating that this area of privacy law would benefit from a preemptive federal statute governing the use of confidential medical information).

[244] *See* HIPAA § 264, Pub. L. No. 104-191, 110 Stat. 1936, 2033 (1996) (codified in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.) (setting forth the timetable for legislation and/or regulations).

By failing to take advantage of the opportunity to assess seriously and propose thoughtful, clear law enforcement rules, HHS has demonstrated that it lacks either the desire, the conviction, or the political will to propose optimal revisions to this area of the law. Further, the statutory foundation of this set of HHS regulations would be HIPAA. This grounding is weak for a number of reasons. First, the goals of HIPAA's Title II center around a desire to speed computerization of health records and to prevent fraud and abuse. The protection of privacy is not the central intent of either HIPAA in general or Title II.[245] Second, as a result of HIPAA's focus on technological and administrative simplification, HIPAA fails to list explicitly law enforcement as an institution to which its privacy standards will apply.[246] The Act simply is not drafted to consider these organizations in such a direct manner. Third, HIPAA does not explicitly discuss the law enforcement use of private medical records as one of the transactions covered by the law.[247]

Given the legal principle that judicial inquiries can often center around congressional intent in passing legislation[248] it seems that HIPAA's pedigree would offer little support for a robust interpretation of any privacy regulations HHS might promulgate.[249] Especially in the contentious and conflicted area of law enforcement access to medical information, it seems that a dubious legislative foundation might undermine the efficacy of any regulations subjected to judicial scrutiny. Statutory law which fails even to define "confidentiality"[250] is certain to fall short of HHS's objective.

---

[245] *See id.* § 261, 110 Stat. at 2021 (stating that the purpose of the Act is to improve "the efficiency and effectiveness of the health care system [by establishing] standards and requirements for the electronic transmission of certain health information"); *see also supra* notes 59-63 and accompanying text (detailing the purpose of HIPAA and noting that privacy protection is omitted from the Act's central purview).

[246] *See* 42 U.S.C. § 1320d-1(a) (Supp. II 1996) (stating that standards shall apply to "a health plan," "a health care clearinghouse," and "a healthcare provider who transmits any health information in electronic form in connection with a transaction" covered by the law).

[247] *See id.* § 1320d-2(a)(2) (listing the transactions to which the standards apply, but omitting law enforcement use).

[248] Language from *Public Citizen v. Nuclear Regulatory Commission*, 901 F.2d 147 (D.C. Cir. 1990), offers some insight into the Court's approach to this issue: "In determining the intent of Congress, we must look to 'the particular statutory language at issue, as well as the language and design of the statute as a whole,' and we must employ traditional tools of statutory construction, including, where appropriate, legislative history." *Id.* at 154 (citation omitted).

[249] Given the guidance in *Public Citizen*, HIPAA's stated intention to "simplify the administration of health insurance" would seem to provide only weak support for a protective interpretation of congressional intent. HIPAA, 110 Stat. at 1936.

[250] *See* 42 U.S.C.A. § 1320d-2(d)(2) (omitting a definition of "confidentiality" and neglecting to provide guidance on who may have access to medical records).

B. *Establish a "Compelling State Interest" Standard and Strict Warrant Requirements Via Clear and Precise Law Enforcement Exceptions*

Although the law is unclear in this area, it appears that Congress cannot simply legislate an explicit Constitution-level interest in privacy. Rather, Congress may only respond to the courts' recognition of a constitutional right or push for a constitutional amendment.[251] Congress, however, can enact legislation that guides judges to give more weight to citizens' privacy interests relative to the law enforcement's need for access, or that altogether alters the framework of the analysis in the judicial context. Specifically, Congress should pass legislation that underscores the importance of the privacy right. It can do so by first establishing a presumptive rule that prohibits all disclosure of certain medical information without prior, meaningful patient consent. Given the practical realities of the need for unauthorized disclosure in certain instances, the law should also clearly and precisely describe a finite list of exceptions.[252] No exception, however, should carry with it a presumptive waiver of the subpoena or warrant requirement. The conditions which merit dispensing with these requirements have been addressed adequately by a portion of Fourth Amendment law.[253] Additionally, obtaining a court order should be dependent upon law enforcement officials' ability to demonstrate that the information sought furthers compelling, legitimate goals that clearly outweigh the privacy interests of the individual.[254]

---

[251] *See* City of Boerne v. Flores, 117 S. Ct. 2157, 2164 (1997) (stating that Congress "has been given the power 'to enforce' [the Constitution], not the power to determine what constitutes a constitutional violation").

[252] There is ample precedent for this approach. *See, e.g.*, Federal Privacy of Medical Information Act, H.R. 5935, 96th Cong. § 131 (1980) (proposing a framework that would have required law enforcement agencies to certify in writing that the information sought was for one of five purposes specifically permitted under the bill). This approach is also similar to that seen in the Rhode Island law discussed *supra* note 207.

[253] Note that such a formulation would not prevent law enforcement from obtaining access without clearing these legal hurdles in every instance. This, in fact, is the legal principle that supports the exigent circumstances rule. *See* 1 HALL, *supra* note 143, § 14.1, at 582-83 ("'Exigent circumstances' is actually not an exception to the warrant requirement. It is but a condition which permits dispensing with the requirement of a warrant for a search as long as the condition exists.").

[254] An example of this type of strict approach is contained in Senator Leahy's proposed 1997 bill governing medical record confidentiality. *See* S. 1368, 105th Cong. § 215(a)-(b) (1997) (imposing a uniform requirement that law enforcement obtain a court order before accessing medical records and necessitating a showing by clear and convincing evidence that the records are "necessary" for the investigation of a "particular violation of criminal law," and that the need for the confidential information outweighs the individual's privacy interests).

Such an approach stands in stark contrast to the mix of legal approaches currently in place, in both the fundamental structure of the principle and the extent to which the principle is expressed here. In the penumbral constitutional privacy right line of cases, which balance privacy rights against the government's need for access, this approach could readjust the balance that has developed to give, in many contexts, too much deference to government justifications for access. In the Fourth Amendment area, this approach implicitly embraces the *Katz* approach, while rejecting the flawed *Miller* arguments.[255]

Since *Whalen* first established and applied a constitutional right to privacy in medical records, the courts have shifted undeniably toward a ready acceptance of almost any stated government interest, including those concerned with law enforcement functions.[256] This imbalance persists despite the fact that significant changes in technology and medical records use have drastically improved the government's ability to collect and analyze confidential data in ways not imagined by the *Whalen* court.[257] Indeed, the courts' ready acceptance of governmental reasoning for this intrusion has led Professor Gostin to conclude that "[a]bsent an improbable upward shift in the courts' level of scrutiny, issues of health informational privacy will be settled in the legislative and executive branches of government."[258] By narrowly defining a finite number of exceptions for law enforcement's access to medical records (and establishing a stricter presumptive warrant requirement), Congress would underscore the importance of the individual's privacy right and help to place into context the nature of government's assertion of its interests.[259] Thus, this strictly limiting structure should help

---

[255] *See supra* notes 150-70 and accompanying text (approving of the *Katz* Court's acknowledgment of a reasonable expectation of privacy and criticizing the *Miller* Court's ownership-based approach).

[256] *See supra* Part II.A.2 (describing the judicial shift toward increased deference to the governmental interest).

[257] *See supra* note 226 and accompanying text (discussing the implications of unfettered data mining in the law enforcement context).

[258] Gostin, *supra* note 8, at 498.

[259] A complementary approach also warrants merit. In addition to listing specific exceptions to the general protections, a bill might also identify certain prohibitions in order to specifically eliminate the potential commission of these acts. For example, Senator Leahy's 1997 proposal prohibited the use of health-related evidence of criminal activity that is collected by law enforcement during the course of an investigation not related to that criminal activity. *See* S. 1368, 105th Cong. § 215(e) (1997) (barring use of any "[p]rotected health information" found in the course of an investigation for purposes other than "action[s] or investigation[s] aris[ing] out of... the law enforcement inquiry for which the information was obtained"). Such a specific prohibition could minimize the chance that the data mining hypothetical discussed *supra* in notes 225-26 and accompanying text might occur.

courts to understand the need for law enforcement to assert a compelling, rather than merely rational, interest.

Similarly, this approach fundamentally alters the current *Miller* analysis commonly employed in Fourth Amendment claims of medical records privacy. Currently, courts relying on *Miller* often make assumptions that lessen the expectation of privacy in one's medical records or reject a privacy claim on the grounds that computerized health information is not the property of the individual asserting the right.[260] As has been noted, this logic flies in the face of prior legal reasoning established in *Katz*,[261] and contradicts the realities of modern health information management.[262] In contrast, the general statutory framework suggested by this Comment embraces the reasoning and structure of the *Katz* analysis, which seems highly appropriate in the medical records-law enforcement context. At its heart, *Katz* offers a two-step inquiry: (1) has the individual exhibited "an actual (subjective) expectation of privacy" in the information at issue, and (2) if yes, is that expectation "one that society is prepared to recognize as 'reasonable.'"[263] The proposed legislative approach recognizes that courts often answer the first question affirmatively in this context, and the narrowly defined exceptions to the general privacy rule would offer substantial guidance in answering the second inquiry. Thus, constructing a statute in this manner would minimize the outmoded and harmful impact of the *Miller* decision in the medical records arena.

It is important to understand that this approach need not hamper law enforcement's efficacy in obtaining information and fulfilling its essential societal role. Most commonly, law enforcement advocates cite the need to respond immediately to imminent potential harms or to identify wrongdoing before it is hidden. As a consequence, law enforcement argues that obtaining a warrant or other judicial approval for access hampers its ability to perform its job.[264] Despite these protests, ample precedent exists for such legal protections of confidential information.[265]

---

[260] *See* United States v. Miller, 425 U.S. 435, 440-42 (1976) (requiring an examination of "the nature of the particular documents sought to be protected in order to determine whether there is a legitimate expectation of privacy concerning their contents" and rejecting an individual's claim where the individual to whom the records apply "can assert neither ownership nor possession").

[261] *See* Katz v. United States, 389 U.S. 347, 351 n.9 (1967) (eschewing the property-based approach to Fourth Amendment protections against unlawful search and seizure).

[262] *See supra* note 161 and accompanying text (noting the considerable criticism *Miller* has received).

[263] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[264] *See, e.g.*, Nat Hentoff, *Just Between You, Your Doctor, and the Police*, THE WASH. POST, Nov. 11, 1997, at A21 (noting that police organizations often object to warrant re-

Moreover, the changes in technology that have given rise to the need for these new privacy protections can also help speed law enforcement's surveillance and investigatory efforts. Inevitable changes in health information management will simplify law enforcement's efforts in this area, further reducing the need for broad access. For example, many observers recognize that the federal government, working in concert with private insurers and providers, will assign patients a universal identifier for health records in the near future, even within the next two years.[266] Such a change would effectively increase the speed and scope of law enforcement's reach into personal health data, furthering the trolling of data for illicit activity, and offering the temptation to seek information via citizens' health records. Judicial review of the purpose and intentions of such an investigation seems an appropriate counterbalance to these improved capabilities.[267]

Finally, although the precision and limited nature of the exceptions has been stressed, one should remember that such exceptions can and will provide law enforcement with the essential capabilities that current statutorily-mandated reporting offers. For example, many current state laws require

---

quirements in this context because "[t]o secure physical evidence . . . there isn't time to get a judicial warrant or deal with rules protecting medical records").

[265] Law enforcement officials cannot access cable television subscriptions and information without obtaining a court order concluding that the information sought is material to the current investigation, and that this conclusion is based on clear and convincing evidence. *See* 47 U.S.C. § 551(h) (1994) (allowing any "government entity" to "obtain personally identifiable information concerning a cable subscriber . . . only if" it meets a "clear and convincing" standard in a court proceeding). Moreover, 18 U.S.C. § 2518, as noted in *United States v. Giordano*, 416 U.S. 505 (1974), embodies a congressional intent to ensure that law enforcement interception of private wire and oral communications occur only with restraint and only where circumstances warrant such intrusion. *See* 18 U.S.C. § 2518 (1994); *Giordano*, 416 U.S. at 515 ("Congress legislated [§ 2518] in considerable detail . . . to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant . . . ."). Section 2518 sets strict requirements regarding the substance of the application to the court, including a complete statement on the other investigative procedures attempted prior to the application. *See* 18 U.S.C. § 2518 (1)(c). Section 2518 also authorizes judicial approval of such a warrant application only when a judge finds probable cause exists under a set of strict requirements and when it appears unlikely that other investigative procedures would succeed. *See id.* § 2518(3) (setting out four specific findings required to support the issuance of a warrant).

[266] *See* Allen, *supra* note 9, at 13 ("The Clinton administration's aim is to help create a seamless nationwide records system that eventually may involve a 'universal patient identifier,' the equivalent of a Social Security number for each patient."). *But see supra* note 9 (discussing recent impediments to this plan).

[267] Technology could help law enforcement in more mundane ways that would help reconcile these new privacy protections with law enforcement's ability to perform its job. For example, in response to the argument that crime-fighting imperatives often obviate the luxury of constitutional protocol, Nat Hentoff quipped, "[W]hy can't current swift technology be used to find a magistrate quickly and get the warrant in time? Magistrates have home phone numbers, and even fax machines." Hentoff, *supra* note 264, at A21.

physicians to report certain injuries, such as gunshot wounds, the contraction of highly contagious diseases, and injuries associated with child abuse.[268] Although the logic supporting many of these exceptions needs review, this review should not create an expectation that the required reporting should be eliminated wholesale within the proposed framework.

C. *Broaden and Strengthen the Principle of Physician-Patient Confidentiality*

Proposed legislation should also expand and invigorate the doctor-patient confidentiality privilege by shifting and possibly expanding current notions of liability in medical records privacy cases involving law enforcement access to such information. Note how establishing liability for those who wrongfully disclose personal health information complements the presumption against disclosure to law enforcement without patient consent. Thus, this suggestion works in tandem with the proposed structure of the law governing law enforcement access by providing another impediment to improper disclosure, from the vantage point of the potential *discloser*. Such a prohibition would be in addition to the penalties suggested for wrongful law enforcement *users* of confidential data, as the *HHS Report* proposes.[269]

Despite the Hippocratic Oath[270] and present-day manifestations of the physician's duty to keep patient information private,[271] doctors often have the discretion to offer law enforcement personnel confidential information.[272] Typically, doctors confronting these scenarios have little guidance

---

[268] *See* Gellman, *supra* note 162, at 274 & n.78 (listing some of the physician reporting requirements that states have enacted, mandating communication between doctors and law enforcement agencies).

[269] For a general discussion of this penalties-based approach, see *supra* notes 241-42 and accompanying text.

[270] 1 HIPPOCRATES 164-65 (W. Jones trans., Loeb Classical Library Series 1923), *reprinted in* ETHICS IN MEDICINE 5 (Stephen Reiser et al. eds., 1977) ("[W]hatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.").

[271] The most recent set of AMA ethics can be found in AMERICAN MEDICAL ASSOCIATION, PRINCIPLES OF MEDICAL ETHICS OF THE AMERICAN MEDICAL ASSOCIATION (1980), *reprinted in* CURRENT OPINIONS OF THE JUDICIAL COUNCIL OF THE AMERICAN MEDICAL ASSOCIATION ix (1981) ("A physician shall respect the rights of patients, of colleagues, and of other health professionals, and shall safeguard patient confidences within the constraints of the law.").

[272] *See* Gellman, *supra* note 162, at 280-84. Professor Gellman discusses the law enforcement hypothetical within a section of his article entitled "Discretionary Disclosures," and notes that when considering the disclosure decision, doctors often find that, "[t]he slippery slope in this area is particularly steep. Once cooperation begins, it is hard to find a place to stop." *Id.* at 286.

in the form of statutes or rules.[273] As has been noted, establishing a clear prohibition on disclosure, like standardization of law enforcement access in general, makes the decision simpler for physicians. This increases the likelihood of compliance, and therefore strengthens privacy protection. Moreover, broadening liability beyond the strict doctor-patient relationship reflects the realities of modern health care delivery and health information management—literally scores of physicians, therapists, nurses, and administrative personnel routinely use or have access to confidential health data. These people also need motivation to defend the privacy interests of patients. This is especially important since law enforcement officials most commonly obtain access to such information through authorized users of the information.[274] Thus, the interaction serves as a logical focal point for the establishment of barriers to improper disclosure.

Admittedly, law enforcement will obtain necessary information from health care providers via exceptions to the presumptive privacy rule. Moreover, exceptions to this confidentiality rule seem warranted in that physicians and therapists should have clear guidance on when their duty shifts from confidentiality to reporting or disclosure, such as to prevent imminent harm.[275] Narrow exceptions in instances such as these should offer an acceptable balance between the protection of privacy and the interests of law enforcement.

D. *Accommodate Technological Advances in the New Law Enforcement Exception*

This general notion is implicit in a number of the recommendations discussed above, but its central importance therein merits a separate discussion of its ramifications. Technology has served as the driver of change in medical records management. It was the impetus behind the passage of HIPAA,

---

273

> Regardless of the decision of a physician on any particular disclosure request—whether the requester is the Secret Service, a fraud investigator, a medical researcher, an intelligence agency, or someone else—the physician generally faces the decision without any meaningful guidance. Basic principles of medical ethics are silent on these issues, and the law is filled with uncertainties about the potential liabilities of physicians who must decide whether to disclose patient information.

Id. at 286-87.

274 *See supra* note 237 (discussing the typical acquiescence by authorized users when responding to law enforcement requests for confidential information).

275 *See supra* note 239 and accompanying text (discussing Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976)).

intended to facilitate further computerization of health records.[276] The effects of technological change lie at the center of the principles guiding the *HHS Report* on health records confidentiality. Going forward, cognizance of the evolving character of technology in this area should help define the contours of any new privacy law.

In particular, technological change dictates that flexible approaches will work best when constructing rules in this area. Therefore, it is not surprising that the *HHS Report* suggests that regulatory and rulemaking authority be established so that developments in technology can be matched by rapid and nuanced changes in the applicable rules.[277] For similar reasons, many commentators have called for the establishment of expert commissions to analyze changes in health information management and use, and to periodically recommend changes to laws and rules.[278]

Arguing for such a commission or group is not novel. However, within this initiative, special attention should be paid to how technological developments impact law enforcement's ability to access private medical information, and rule modifications should be suggested accordingly. For example, both the implementation of universal health identifiers[279] and the creation of technology to promote the segregation and security of information within a patient's total medical record[280] could impact how law enforcement should be allowed to access this information, and which items within the record it should see. Particular emphasis on this specific area of responsibility for an oversight committee or federal agency charged with rulemaking accomplishes two goals: (1) it creates a mechanism for early understanding of how future technological changes in health information might drive needed changes in the laws governing police access to this information toward preserving individuals' privacy interests in this area, and (2) it further underscores the importance of citizens' privacy interests vis-à-

---

[276] *See supra* notes 62-63 and accompanying text (noting that the purposes of HIPAA focus on improving the efficiency and effectiveness of health care delivery).

[277] *See* HHS REPORT, *supra* note 18, at pt. II.I.1 ("We recommend that there be authority to . . . develop information and technical guidance for protection of health information; and develop technology to implement standards regarding health information.").

[278] *See, e.g.*, Schwartz, *supra* note 13, at 340-42 ("The protection of informational self-determination in an age of rapid technological change mandates the creation of a governmental body with the institutional expertise and continuity of interest to understand the impact of changes in this area and draw attention to the need for improvements in legal regulation.").

[279] *See supra* note 266 and accompanying text (acknowledging the goal of creating unique patient identifiers).

[280] *See* OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 178, at 97-98 (1993) (noting that "access control software" can determine not only "who can use the system," but also "what system resources they can access").

vis law enforcement access to confidential medical records in any judicial balancing.

Interestingly, law enforcement officials have taken the converse position, insisting that because of the rapid technological change that characterizes health information management and record keeping, no new restrictions should be placed on law enforcement access at this time.[281] Such an argument presupposes that the pace and nature of this change will slow and stabilize at some point in the future, which seems to be an ill-conceived notion at best. The changes of the past decade have weakened privacy protections, and it is clear that this process will continue if not addressed. The establishment of stronger rules, in addition to an oversight body for studying future changes and suggesting new solutions to incipient problems, is clearly preferable to simply waiting for a time that may well never arrive.

CONCLUSION

The conclusion to be drawn from this Comment is a simple one: Societal, technological, legal, and moral justifications exist for Congress to enact clear, robust legislation governing law enforcement's use of individually identifiable medical information. Changes in the delivery of health care, combined with changes in the collection, use, and sharing of health information, drive the need for changes in how law enforcement obtains access to and uses citizens' health records. Effective law enforcement is essential to a well-ordered and beneficial society, and this role requires law enforcement's use of medical information. At the same time, moral and legal principles demand meaningful privacy protection of health information, not just for the benefit of society, but for each individual's betterment as well.

The Department of Health and Human Services report to Congress, "Confidentiality of Individually-Identifiable Health Information," fails to recognize that these two competing issues must be considered jointly when Congress debates privacy legislation for medical records. Although the *HHS Report* acknowledges that changes in health care and technology drive the need for change in many areas of medical records privacy law, and that law enforcement must be able to perform its role as investigator and prosecutor, the *Report* does not adequately address the conflicts between these two aims. Instead, the *Report*'s recommendations on this subject indicate an abdication by HHS of its duty to weigh these conflicting aims and create

---

[281] *See* HHS REPORT, *supra* note 18, pt. II.D.10 (stating that the imposition of additional restrictions on law enforcement's access to medical information databases would be inappropriate "[u]ntil more experience is gained with the nature and speed of computerization of these records").

potential reconciliations between them. Indeed, rather than getting the balancing wrong, it seems that HHS simply returned this controversial subject to Congress, wherein ultimate responsibility for the form and content of future law in this area lies.

The critique of the law enforcement exception contained in the *HHS Report*, then, is also implicitly a critique of the failings of current law in this field. The arguments that compose this critique, and resulting recommendations for fixing the HHS recommendations, are therefore founded upon the perceived weaknesses of the present legal framework. As Congress returns to medical records privacy in the coming months, it must consider many of the issues at stake in the law enforcement use of health information; for the concerns, interests, and rights in this seemingly narrow subsection of the debate over medical records privacy, in fact, loom largely over the ultimate strength of protection that any new law will provide. Without a narrowly and more clearly defined law enforcement exception, the government's ability to reach far into our private medical records will become more than just a chilling movie screen fantasy.

* * * * * *