33 RULJ 617
33 Rutgers L.J. 617
(Cite as: 33 Rutgers L.J. 617)

Rutgers Law Journal
Spring 2002

Article

***617** CONFIDENTIALITY IN CYBERSPACE: THE HIPAA PRIVACY RULES AND THE COMMON LAW

Peter A. Winn [FNa1]

I. Introduction

Few types of information are more sensitive than our medical records; and yet, few types of personal information are more commonly disclosed. The reasons medical records are disclosed are usually legitimate. Disclosure must take place so that adequate treatment decisions can be made, to insure correct insurance payments, for proper health oversight, for medical research, and to protect the safety of the public. However, when improper disclosure of medical information takes place, it can cause great harm to patients and can seriously undermine the bonds of trust between doctors and their patients.

Traditionally, the legal mechanism used by courts to balance the need to protect patient information against the need for disclosure has been the common law tort of breach of confidentiality. On April 14, 2001, the federal Standards for Privacy of Individually Identifiable Health Information [FN1] (the "HIPAA Privacy Rules" or the "Rules") became effective, promulgated by the Department of Health and Human Services under the authority of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). [FN2] Underlying the decision to promulgate the Rules was a lack of confidence in the ability of traditional common law doctrines to protect personal health information in an age when medical records are no longer kept in locked file cabinets in doctors' offices, but exist in electronic form in the context of vast health information networks accessible by hundreds of different persons fulfilling various ***618** disparate functions. [FN3] Because the increased access to electronic personal health information increases the danger of harmful disclosure and misuse of that information, Congress, in enacting HIPAA, authorized federal regulatory protections for personal health information. [FN4] The resulting Rules establish a federal floor of protections similar to those provided by state medical confidentiality laws, but do not preempt state laws which provide for greater protections. The Rules also establish a set of fair information practices giving patients certain rights of notice, access, security, and consent with respect to disclosures of their personal health information that were not ordinarily provided under traditional common law doctrines of confidentiality.

The HIPAA Privacy Rules have been criticized for two important perceived shortcomings. First, the Rules create an administrative enforcement mechanism, but they do not create a federal private cause of action for individuals who are injured by a violation of the Rules. Second, the Rules only subject to legal sanction healthcare providers, health plans, and clearinghouses--what the Rules call "Covered Entities." [FN5] The Rules do not subject to legal sanction any of the numerous entities whose access to personal health information has exploded with the increased use of electronic health information--that is, businesses which provide legal, accounting, administrative, management, and oversight services to healthcare providers and health plans--what the Rules call "Business Associates" of covered entities. [FN6] This is considered particularly troubling because such business associates appear to have been responsible for many of the abuses of personal health information that led to the enactment of the Rules in the first place.

Many leading healthcare scholars share with the drafters of the Rules a lack of confidence in the ability of the common law to maintain the ***619** confidentiality of personal health information in an electronic age. [FN7] This Article argues that the lack of confidence in common law protections is due to a mistaken focus on the need to protect a "right of privacy" in sensitive private information instead of on a need to protect relationships of trust. This theoretical mistake leads in turn to the conflation of two different torts: breach of confidentiality and invasion of privacy. While the invasion of privacy torts tend not to be effective in addressing most common types of improper disclosure of health information--that is, those caused by negligence--the breach of confidentiality torts are more effective in this context--a fact that should not be surprising, given that breach of confidentiality was a doctrine originally designed to address precisely the problem of improper disclosure of sensitive medical information. This Article argues that the common law tort of breach of confidentiality can continue to provide an effective private remedy even in a world in which most personal health information has become electronic.

The failure of the HIPAA Privacy Rules to create a private federal remedy does not imply that the Rules will exist in a parallel federal universe with no influence on state common law doctrines. This Article argues that the HIPPA Privacy Rules, although federal, are likely to be adopted by state common law courts to extablish a national minimum standard for liability for breach of confidentiality under state law. Like the HIPAA Privacy Rules, most early state statues and ethical rules establishing a duty of confidentiality did not create a private right of action for their violation. However, these apparently toothless statutes and ethical rules constituted the basis of the early cases establishing the common law tort of breach of confidentiality. While it does not appear likely that courts will use HIPAA to imply a federal private cause of action for breach of the Rules, it does appear that the minimum federal standard established by the HIPAA Privacy Rules are likely to be adopted in private state actions for breach of confidentiality ***620** as establishing the duty whose breach is the predicate for the underlying tort claim.

With respect to the second perceived weakness of the Rules, because the breach of confidentiality tort traditionally requires that the patient be in a professional or contractual relationship with the person responsible for the wrongful disclosure, and because many harmful disclosures take place by entities such as business associates who are not in such a relationship, the breach of confidentiality tort has been viewed as unable to address the problems caused by the widespread dissemination of electronic health information among "downstream" users not in a relationship of confidentiality with the injured person. [FN8] In this context, this Article reviews a series of innovative and important cases in which courts have found liability against "downstream" users of health information under breach of confidentiality theories, even though the defendants were not in a professional or contractual relationship with the patient. The Article then compares these common law developments with provisions of the HIPAA Privacy Rules which provide that before a covered entity may grant access to personal health information to a business associate, the covered entity must obtain a written contract from the business associate promising to adhere to the same confidentiality standards as the covered entity. The Article argues that, under the developing case law, such federally required agreements with business associates, while ostensibly creating no legally enforceable duties other than between the contracting parties, are likely to facilitate the establishment of claims for breach of confidentiality against business associates by patients for

misuse of their personal information in spite of the lack of a professional or contractual relationship--in effect, creating a "chain of trust."

***621** The final section of this Article addresses the question whether actions for breach of confidentiality applied to business associates in such a "chain of trust" can survive First Amendment scrutiny. Many restrictions on the free flow of information designed to protect a "right of privacy" in sensitve personal information have faced intense scrutiny under the First Amendment. In contrast to restrictions on disclosure based on a "right of privacy," restrictions on disclosure based on contractual or professional relationships of trust receive more favorable treatment under standards set out by the Supreme Court in Cohen v. Cowles Media Co. [FN9] This Article argues that because the tort doctrine of breach of confidentiality does not create rights of privacy in information, itself, but protects information only in the context of well-defined relationships, it is likely to survive critical First Amendment review.

II. Health Information: Protection and Disclosure

A. The Importance of Protection of Health Information

Patients are highly sensitive to disclosure of their health information. The disclosure of certain types of adverse health information can have a powerful, often destructive, impact on the person who is the subject of that information. Many diseases have a social stigma that no laws against discrimination can banish. Even the disclosure of some medical conditions that are not contagious and have no adverse impact on others may damage an individual's reputation with colleagues, friends, and family. For instance, the knowledge that an individual has cancer or is HIV positive may cause others to shun that person. In certain cases, disclosure of medical information may result in the loss of a job, the alienation of family and friends, the loss of health or life insurance, public humiliation and, in certain circumstances, irreparable psychological trauma. Moreover, health information often involves intimate and personal facts, with a heavy emotional overlay. Certain medical conditions may threaten an individual's self-worth and dignity, or affect his or her sexuality or bodily functions. The simple fact is that disclosure of such highly charged personal information can matter greatly to the affected person simply because that information is so intimate and so personal.

***622** The dangers associated with disclosure of personal health information have a strong practical impact on the relationship of trust between a patient and a physician. The doctor must trust the patient to give full and truthful information about her health, symptoms, and medical history. The patient must trust the doctor to use that information on behalf of the patient and to keep the information confidential. If a patient believes that a doctor will not keep his or her medical information confidential, the patient may not be willing to tell the truth about sensitive personal matters. If a doctor is not provided truthful information, the doctor will be unable to render proper care to the patient, and the doctor's ability to treat the patient may be impaired. Because the protection of healthcare information is central to the ability of healthcare professionals to do their jobs, health information must be protected in order to maintain the integrity of the relationship between patient and healthcare provider.

Physicians, nurses and other healthcare providers have long known that fear of disclosure of health information may cause people to withhold information, to lie, or to avoid treatment altogether. Accordingly, beginning at least as early as the ancient Greek physician Hippocrates, healthcare providers have maintained a strong presumption against disclosure of their patients' health information. [FN10] The general rule of confidentiality for medical professionals continues to be strongly emphasized by providers today. [FN11]

B. Disclosures of Health Information

Although confidentiality is a central concept in the provision of healthcare, health information must also be disclosed for many purposes. These types of disclosures can be organized into four general categories or zones: (1) disclosures

that are made between healthcare providers to enable the delivery of primary healthcare; (2) disclosures to payers to ensure the payment of claims, to ensure the quality of care provided and effective oversight of the payment system; (3) disclosures that are made to further public purposes, including public health, law enforcement and for research; ***623** and (4) disclosures that take place for private purposes unrelated to treatment, payment, health oversight, research or other public purposes. [FN12]

C. Disclosure for Purposes of Treatment

In the first zone, disclosure must take place for purposes of treatment. In order to properly treat their patients, doctors and other healthcare providers must share with other providers, such as nurses, druggists, lab technicians, and other medical personnel, sensitive medical information about their patients. Such disclosures among and between medical professionals appear to have taken place since the time of the first Greek physicians and are necessary for proper treatment, as well as for the training of new physicians. [FN13] In addition, within the context of a healthcare facility, such as a hospital, many people not directly involved in providing patient care also may have access to a patient's medical records and other personal information. In most hospitals, clinics and other healthcare facilities, patient files follow the patient to the ward where the patient is located. As such, personal health information pertaining to the patient may be seen by nurses and other hospital personnel on duty in the ward--even hospital cleaning staff. Financial information relating to the patient will be maintained in the hospital's billing office, drug orders will be maintained by the hospital pharmacist, radiological records in a separate storage area, and so forth. Hospital employees will typically have general access to patient records because of their job functions, even if they are not involved in the treatment of the patient.

Hospital stays are also notoriously non-private affairs. Doctors and the staff of a hospital typically coordinate services at open nursing stations, discuss a patient's condition over the phone with the patient or other health care provider, even if other people are nearby, discuss lab tests with a patient or other provider in a joint treatment area, call out a patient's name in a waiting room or discuss a patient's condition during training rounds in an ***624** academic or training institution. Patient charts are maintained at bedsides, prescription vials maintained on night tables, and x-ray light boards are left in open view. As a practical matter, a patient usually has very little privacy in a hospital. The patient is scantily clad in a hospital gown, has to share a room with other patients, and may be observed semi-clad and in various intimate functions by other physicians, nurses, and hospital staff, as well as hospital visitors. Paradoxically, this broad absence of privacy co-exists with a culture among medical professionals and medical staff that sensitive personal information observed in the context of a hospital stay is not to be disclosed outside of the context of the medical treatment arena. Medical providers are generally aware about the potential harm that may result from incidental disclosures of sensitive patient information in the routine day-to-day operation of a hospital. However in the somewhat hectic environment of a hospital, confidentiality often become subordinated to the need of doctors, hospital staff, patients and their families to communicate in an effective and convenient manner. In most cases, such routine breaches of confidentiality result in disclosures largely to people who are uninterested in using the information. Accordingly, at least until the introduction of computer networks, the potential for harm from such improper disclosures has been limited and the system could tolerate the "slippage" in confidentiality.

The introduction of networked computer information systems, discussed later in this Article, appears to have dramatically narrowed the tolerance of the system to such "slippage." In the loose environment of a health care provider, a 13-year-old daughter of a hospital staff member can access patient medical records from a computer terminal, and, as a prank, call the patients and inform them they are HIV positive. [FN14] Celebrities admitted to hospitals are faced with a virtually unlimited number of people with the ability to "peep" at their medical records--sometimes, as in the case of Arthur Ashe, with tragic consequences. [FN15] As a consequence of such incidents, health care providers and policy makers are being forced to recognize that "slippage," which may have been harmless in the past, now may have unacceptable consequences.

***625** D. Disclosure for Payment and Health Oversight

1. Payment

If medical treatment is paid for in cash by the patient, it is relatively easy to control the disclosure of medical information outside of the zone of treatment. With the inception of third-party health plans (such as private insurance companies, employer-funded plans, or government health benefit programs), which pay in whole or in part for a patient's medical expenses, disclosure of medical information outside the zone of treatment has become much more widespread.

The standard health insurance claim form used by physicians as well as many other health care providers contains numerical codes listing diagnosis and treatment, as well as much other sensitive personal information about the patient. [FN16] In order to receive an insurance payment, a physician must typically disclose not only the name and address of the patient and the amount of the charges, but the most critical medical information about the patient of all--the patient's diagnosis and the treatment provided. A health insurance plan cannot pay for medical treatment without knowing what treatment was provided and that it was appropriate for the given diagnosis. Unless a patient pays for healthcare without insurance, this form of disclosure is generally viewed as necessary and proper.

However, within the payment process, large numbers of individuals have access to this information. Private insurance plans typically retain third-party administration companies to process the claims for payment. Governmental payers such as Medicare and Medicaid retain private carriers and intermediaries who perform similar functions. Physicians and hospitals, themselves, often hire individuals or outside billing companies to submit bills and collect payments from insurance payers. Hospitals, nursing homes and home health companies may retain independent professionals to review medical records prepared by physicians and nurses and determine codes for ***626** the appropriate primary and secondary diagnoses, as well as the appropriate diagnostic-related groups for the billing of the treatment. Accountants and other professionals may be hired to prepare cost reports. In spite of the extent of routine disclosure that takes place within the payment review process, most professionals involved in the processing and payment functions appear to take seriously their obligations to maintain patient confidentiality and maintain a strong culture of respect for these values. Like their counterparts in the area of treatment, however, the introduction of computer networked information systems has caused the number of individuals with access to patient medical records to explode. While formerly insurance companies may have hired trained nurses to process health claims, the introduction of computer processing programs has allowed many claims administration companies to hire employees with little more than a high school education and little training or experience in confidentiality. With more untrained people having access to medical information comes new dangers to confidentiality and the integrity of the health care payment system.

2. Oversight

While the vast majority of payments by health plans take place virtually automatically based on numerical diagnosis and treatment codes, private and governmental plans periodically review the patient's actual medical records, in whole or in part, to ensure that the treatment provided is medically necessary or of appropriate quality. Independent health care professionals are often retained by both insurance payers and by health care providers to conduct reviews of the quality of care provided patients and whether the care provided was medically necessary. In such reviews measure hospitals and other medical providers against established norms for use of the facilities, length of stay, patient-staff ratio, and so forth to ensure that the care provided is in conformance with established norms of competence. Many different organizations perform these functions, including the healthcare organizations themselves, health insurance plans, accrediting agencies and public health agencies. State professional licensing authorities have the authority to review medical records to monitor the quality of care rendered by physicians, nurses, hospitals, and other licensed medical providers. [FN17] These organizations often subcontract with Peer Review Organizations, ***627** which retain independent physicians to conduct

extensive reviews of individual medical files to monitor and oversee treatment provided by physicians, hospitals, pharmacists, nurses, home health agencies, nursing homes, and many other healthcare providers. [FN18] Typically such reviews may involve the patient's entire medical file. While some disclosure of sensitive personal health information is critical to appropriate oversight of any properly functioning healthcare system, such oversight involves risks of improper disclosure as well. When oversight takes place in the context of networked information systems, it is often difficult for patients to separate legitimate disclosures from illegitimate disclosures. For instance, a pharmacy benefit management company ("PBM") may be hired by an insurance payer to adjudicate and pay claims as well as to manage a formulary. [FN19] The PBM may suggest less expensive generic medications on behalf of the payer, as well as warn pharmacists and physicians of adverse drug interactions or otherwise contraindicated medications. If the prescribing pharmacist is not aware of the other contraindicated prescription the patient is taking, which may happen in the case of an elderly or impaired patient being seen by more than one physician, the PBM may become a critical secondary safety net to identify this information. On the other hand, a patient, who receives communications from a PBM appearing to market a drug for their medical condition, may rightly be concerned by what appears to have been a breach of confidentiality represented by that disclosure. The patient may not be in a position to determine whether the PBM is improperly using the patient's confidential prescription information to conduct marketing activities on behalf of a drug company or whether the PBM is legitimately acting on behalf of the patient's insurance payer to inform the patient about the possibility of substituting a lower cost or more effective alternative to the drug prescribed by the physician. [FN20]

Finally, within the area of health care oversight are private and governmental fraud detection programs. In 1992, the GAO has estimated ***628** that fraud and abuse accounts for 10% of the total United States expenditures on healthcare. [FN21] In 1999, the United States spent in excess of one trillion dollars per year on healthcare and by 2010 is estimated that spending will rise to 2.3 trillion dollars. [FN22] Given the massive amount of fraud that pervades the system, it is critical that energetic fraud detection efforts continue. In fraud reviews, it is not uncommon for the patient's entire medical file to be reviewed by the fraud investigator, including the notes of the physician, radiological and laboratory reports, drug prescriptions, and other treatment records. Although information acquired by a health care fraud investigator is usually subject to the confidentiality requirements during the course of the investigation, [FN23] prosecutors and investigators are not always as careful as they should be to redact patient names when presenting evidence of the fraud in the course of a public trial.

E. Disclosure for Public Health and Safety and for Research

1. Public Health and Safety

It is impossible, given the scope of this Article, to fully describe all instances in which the law requires disclosures of personal medical information for public purposes. However, as the following examples indicate, many disclosures of sensitive health information are routinely made to insure public health and safety without the consent of the subject of the information.

Public health officials, such as local health departments and national organizations such as the Centers for Disease Control and Prevention, gather data on communicable diseases in their work to prevent epidemics. They also collect and analyze behavioral information regarding alcohol and drug use, smoking, exercise, and sexual practices. [FN24] States mandate reporting of a wide range of infectious diseases, injuries, and other health conditions to public health agencies. [FN25] They operate in conjunction with law enforcement ***629** authorities to track and monitor all prescriptions of certain scheduled drugs to prevent over prescription of addictive drugs and diversion of controlled substances. [FN26] Public health authorities also have broad surveillance powers in the context of epidemics such as plague, cholera, smallpox and yellow fever. The HIV epidemic in the 1980's and 1990's saw the institution of mandatory reporting and partner notification requirements by states in the interests of public health and safety. [FN27] Most recently, public health

authorities have exercised broad power to review medical records in the context of bio-terrorism attacks. [FN28]

The requirement of disclosure of health information for public purposes is not limited to public health authorities. In most states, medical providers are required by statute to disclose to law enforcement instances of gunshot wounds, child abuse, or other instances where a threat to public safety exists. [FN29] In the absence of express statutory mandates, some courts have found a similar common law duty, founded on reasons of public policy, to disclose patient information when physicians become aware of such information that, if not disclosed, could result in physical harm or death to members of the public. [FN30] In the famous case of Tarasoff v. Regents of University of California, [FN31] the Supreme Court of California imposed a common law duty on psychotherapists to disclose threats of harm by their patients to third parties in limited circumstances. [FN32] While not all states have adopted the Tarasoff doctrine, nearly all states place an affirmative duty upon physicians to report the treatment of gunshot wounds and poisonings in which there is a threat of physical danger to the general public. [FN33] Many ***630** states have statutes requiring disclosure by a physician of suspected physical or mental abuse of a child or an elderly or mentally disabled person. [FN34] Likewise, many states require physicians to notify a spouse or known contact of a person having HIV infection or AIDS. [FN35] Most schools and camps for children require disclosure of vaccinations and other health conditions. In the context of civil and criminal litigation, disclosure is required to ensure just adjudication of disputes.

Disclosures required as a matter of public policy can sometimes be extremely controversial. For instance, partner notification and reporting requirements in the context of sexually transmitted diseases or HIV prevention programs have generated bitter controversy. [FN36] Such legally mandated disclosures generally are the result of a public debate and reflect a balancing of the importance of protecting the relationship of trust between patients and providers against the importance of other important public policies served by the required disclosures. In general, however, courts have shown themselves extremely reluctant to interfere with statutes and regulations granting to public health authorities the authority to acquire and use personal health information, provided that the government articulates a legitimate societal purpose such as protecting public health, and employs reasonable privacy and security measures preventing secondary disclosure of the information for other purposes. [FN37] On the other hand, the advent of computerized information networks in the field of public health has placed strains on the scattered and sometimes confusing confidentiality provisions in state law. To address these concerns, respected scholars such as Lawrence O. Gostin have called for the enactment of a Model State Public Health Privacy Act that balances the social good of data collection and the individual good of privacy. [FN38]

2. Research

The problem of respecting confidentiality in the context of medical research often involves extremely difficult trade-offs between the public interest in improving medical science and the rights of the affected ***631** individuals. Access to medical records is, of course, often necessary for medical researchers to enhance general scientific knowledge or improve treatment protocols. However, the expansion in the types of information that can be accessed through an electronic information network has caused a reevaluation in the somewhat loose procedures that heretofore have governed the research community's access to medical records.

For federally funded or authorized research, questions of confidentiality are governed by Institutional Review Boards ("IRBs") at the medical institution. [FN39] While the role of IRBs is beyond the scope of this Article, in general IRBs are required to have at least five members, one of which is from outside the institution. [FN40] IRBs review the benefits and risks to subjects of proposed research and the importance of knowledge that may reasonably be expected to follow, and examine the process by which investigators explain relevant issues in order to obtain informed consent, if possible, from the research subjects. [FN41] In recent years, the IRB system has been subjected to criticisms in that there is no minimum level of privacy protection that is required in the context of the research, and--perhaps the most important

concern--IRB review and approval is not required for privately funded research. [FN42]

F. Private Disclosures Unrelated to Treatment or Payment

In the private sector, disclosures can take place for purposes unrelated to treatment, payment, or health oversight. Perhaps the two common examples of such private disclosures take place in the contexts of insurance and employment.

1. Insurance

In the context of insurance, disclosure of medical information is often needed by insurance carriers in order to make appropriate underwriting decisions in order to properly price policies for life, health, disability, and ***632** other types of insurance. Insurance companies often require potential customers to permit them access to medical records from previous doctors and healthcare providers. They may also employ their own healthcare providers who examine the patient. Depending on the nature of the insurance policy, these exams can be quite detailed, or can be a brief physical examination and the collection of a blood sample. While insurance companies obtain such information with the consent of the insured, the insured has little choice in the matter if he or she wishes to purchase life or health insurance.

Insurance companies also engage in the controversial practice of placing health records thus obtained in a central database called the Medical Information Bureau ("MIB"). The health information collected at the MIB is available for inspection by other insurance companies. The ostensible purpose of such a central database of health records is to prevent insurance fraud. [FN43] However, insurance companies that are members of the MIB have access to large amounts of personal medical information of individuals. Member insurers are officially forbidden from using the information contained in an MIB file as the basis for denying insurance, but only as a basis for further investigation. [FN44] As a practical matter, of course, further investigation may well lead to the denial of coverage if a misrepresentation by a prospective insured is discovered. MIB member insurers contractually agree to a number of specific confidentiality requirements. For instance, MIB reports may not be used for purposes unrelated to insurance underwriting (for instance, use in the context of an employment application). [FN45] Although the MIB audits its members to ensure compliance with these requirements, the quality and effectiveness of such oversight rests exclusively in the hands of the MIB, and the widespread availability of large amounts of individual medical records to insurance companies remains an issue of considerable concern. [FN46]

***633** 2. Employers

Disclosures of personal health information also take place when employers require employees to take a physical by a company physician either in the context of employment decisions or in the context of employer-maintained "wellness programs." The purpose of these wellness programs, however, is to improve the health of employees, and to monitor employees who may have problems of substance abuse or psychological problems who might be a danger to their co-workers. These "wellness programs" often result in considerable health information being obtained by company physicians. Like the insurance physical, the information obtained by company physicians was usually limited in scope to those health matters with some relevance to job performance. Still, the ability of employers to use this personal health information for other purposes has also raised questions, and occasionally litigation. [FN47]

The advent of the Employee Retirement Income Security Act of 1976 (ERISA) [FN48] led to the replacement of private independent health insurance carriers by health plans funded by employers as the principal financing vehicle for the payment of private healthcare. [FN49] The employer, as the plan sponsor, is responsible for payment of the health claims; the "insurance company" is usually charged only with processing the claims according to the terms of the plan document. [FN50] As plan sponsor, an employer has access and can review claims paid by the health plan. Since payment

data necessarily includes treatment and diagnosis, employers have access to this information. Employers often maintain a company file of all medical insurance claims for each employee at the company. A study of employers found that half of employers used employee health information to make employment-related decisions. [FN51]

***634** Employers who access information about an employee's health from their employer sponsored health plans obviously are in a position to use that information to make decisions that are adverse to the employee's employment interests. This creates what may be the most pressing of all issues regarding health care confidentiality. As more and more employers access employee medical records, employees may feel that they no longer will be able to confide in doctors and other health care providers for fear of adverse employment consequences. State confidentiality standards applicable to the improper use and disclosure of personal health information are pre-empted by ERISA, which currently lacks any equivalent provisions for the protection of patient confidentiality and privacy. [FN52] Accordingly, it appears that only a federal solution can address the threat to health care confidentiality created by employer access to protected health information.

III. Revolution in Electronic Health Information

A. Benefits of the Use of Electronic Health Information

In recent years, more and more healthcare providers and payers have adopted computerized medical information systems. The use of electronic health information holds great promise to dramatically improve the quality of treatment that can be provided, but it has also dramatically complicated the problem of protecting sensitive information.

Using electronic medical records in standardized formats, physicians are able to focus more efficiently on critical information in laboratory results, radiology reports, progress notes, and other reports than was the case previously when they had to collect and review disparate paper records. Electronic medical records also may be structured in hypertext, permitting relevant information to be expressed with flexibility impossible with written medical records. Electronic medical records permit more effective quality assurance; reviewing personnel can quickly determine whether appropriate medical protocols are followed and whether appropriate standards of care are being followed. Computer programs can be designed to catch and flag human errors, particularly with respect to drug therapy, identifying contraindicated medications, and correcting mistakes in prescribed dosages. Electronic medical records permit routine medical treatment to take place at different locations, by different physicians with different specialties and at ***635** different hospitals. Even routine lab tests and radiological procedures are now performed and interpreted by enterprises located far away from the hospital or doctor that orders the tests. Within a network of electronic information, patient information may be shared among these sites efficiently and rapidly, offering the possibility of an integrated, centralized database that can hold the patient's entire medical history, from childhood pediatric visits to geriatric records. The remote access to electronic medical records permits doctors to check up on their patients from home, or consult with experts in distant parts of the country. Travelers may be treated by doctors who can access the patient's medical record on-line and rapidly be able to make a careful and informed diagnosis, despite having no prior relationship with the patient.

In addition to revolutionizing the treatment process, electronic health information networks have also dramatically changed the system of payment and oversight for health care. Computer networks make possible far more extensive efforts by payers to control and manage medical costs. This is good and bad. On the one hand, electronic medical records permit more effective cost controls by payers, identifying medically unnecessary tests and procedures, and isolating physicians who order an unusually high number of lab tests or whose patients have abnormally high rates of hospitalization. On the other hand, this also tends to result in far more extensive requirements for the pre-approval of services and a greater tendency by payers to micro-manage the practice of medicine.

The use of electronic health information networks has also permitted far greater specialization in the payment and

oversight system than ever before. Instead of a single claims processing center, payers have specialized into claims administration companies, utilization reviewers, pharmacy benefit managers, and a host of other sub-specialized organizations. Program integrity units operating in conjunction with law enforcement officials can track and access databases of health information to more effectively identify and prosecute healthcare fraud. Access by medical researchers to vast amounts of computerized patient data promises to revolutionize medical science and research, particularly in the context of recent developments in genetic studies. [FN53] Likewise, electronic medical records permit public health ***636** authorities more effectively to identify, monitor, and forecast health threats; more effectively respond and intervene; and evaluate the effectiveness of various public health programs.

B. The Problem of the Protection of Electronic Medical Records

Just as the flow of electronic health information provides dramatic benefits, it also dramatically increases the amount and extent to which personal health information may be disclosed. Quite simply, the more the flow of electronic health information is facilitated, the more confidentiality, privacy, and security are threatened. Of course, the tension between the potential benefits and potential risks of electronic information is not unique to the field of health care.

In general, as our society makes a transition from an age in which records were predominately on paper to an age of electronic information, it has failed to develop effective information management and control structures. The proliferation of access to electronic information has outstripped the former structures that previously controlled access to the information and protected it. As the capacities of hardware, software, and communications networks increase, and as the costs of accessing information correspondingly decrease, information can be accessed and used in ways that were previously impractical. However, at the same time, the opportunity to misuse information also increases, and it is more difficult to control such information abuses. As the management of information becomes more and more ineffective, concerns about privacy and confidentiality begin to limit the potential benefits available from the new forms of electronic information. The tension between the free flow of information and the potential harms from the disclosure of such information exists throughout the field of electronic information. [FN54]

In a world of paper-based information, many forms of information may not have needed protection by legal privacy rules because they retained a high degree of practical privacy because of the inconveniences of retrieving the paper records. For example, personal information that was previously stored in public record keeping systems at local, state, and federal agencies, courts, department of motor vehicles, county records offices, electoral commissions, while theoretically accessible by any member of the general public, was, as a practical matter, restricted by the need to fill out forms, pay fees, and wait in line for record searches. While it was possible for a private ***637** investigator to compile a profile of an individual in this manner, doing so was time consuming, inconvenient and often expensive. Because of the substantial costs of compiling this information, few would access the records without a good reason to do so. While technically "public," the cost of accessing the information created in practice a privacy default. With the transformation of paper information to electronic form, the privacy default has now been eliminated; the previous public character of the information under the legal regime has become a public default in practice. In a world where more and more public information is now on-line, a profile can be built of the individual who is a subject of this information in a matter of minutes, at minimal cost. [FN55] As more and more "public" information becomes available at lower and lower costs, concerns increase about the risk to privacy that did not exist in the context of the world of a paper record keeping system.

The increased accessibility of electronic health records has followed a similar course. Before personal medical records were in electronic form, an individual's healthcare information might be in multiple locations, poorly aggregated and identified by a different number or identification scheme in each place, and incomplete. While this information was less useful than its electronic counterpart, by the same token, it received a privacy default level of protection, simply because it was so hard to get to and link into a coherent picture. The very inefficiencies of paper-based medical records made the

legal standard of confidentiality relatively easy to apply and enforce. A single individual would typically be responsible for record keeping and be identified as the custodian of records.

When personal health information is transformed into an electronic medical record, especially in a networked computer system where the number of people with access to the record dramatically increases, the management of the use of electronic medical information becomes correspondingly more difficult. Responsible management of electronic medical records is particularly problematic given that there are so many legitimate and legally permitted disclosures of such information. As medical information is transformed from paper-based to electronic, the danger that information will be misused is not restricted to healthcare providers, but extends outwards to payers and to the many specialized companies ***638** performing claims processing and utilization review functions for them, as well as to the public health departments, peer review organizations, licensing agencies, law enforcement, and other private entities with access to the information.

In the days of a paper record, inadvertent disclosures of medical files to hospital personnel without a role in the patient's care may have been tolerated since the likelihood of harm to the patient was quite low, and the burdens greater controls placed on convenience and communication were quite high. [FN56] With thousands of employees at an HMO having the power to tap into patients' health treatment records from any number of computer terminals, the comfort level that previously accompanied inadvertent disclosures of personal information appears to have begun to erode. [FN57] There may have been grudging tolerance of the practice of businesses accessing the health records of their employees from the payment records of employee group health plans when the abuses of that practice were limited by the practical limitations of paper based records. In an age of electronic medical records where "slippage" in a system of confidentiality is much less forgiving, that tolerance appears to be evaporating.

As patients become aware that the world of locked file cabinets in their doctors' offices has been replaced by a world in which electronic information is accessible from countless computer terminals throughout the world, a deep-seated ambivalence has begun to develop about whether easily accessed and accurate medical information is a benefit or a curse. This ambivalence threatens the basic institution of trust between medical provider and patient, and raises concerns that patients will begin to adopt strategies of deception or treatment avoidance because of concerns about confidentiality. Thus, concerns of confidentiality may well have begun to operate as a practical limit on the potential benefits of electronic medical information. [FN58] The benefit of the electronic medical record derives from the fact that electronic information can and does flow freely. However, as stories of abuses from improper access to electronic health information circulate more ***639** and more frequently, the danger arises of loss of trust in the integrity of the health care system itself. [FN59] When such concerns cause patients to provide misinformation to healthcare providers, or causes providers to provide misinformation to payers to protect their patients, the potential benefits of the electronic medical record cannot be realized. In the age of paper medical records, disclosures of personal health information that may have taken place among medical personnel, insurance payers, and public health authorities did not apparently undermine the trust of patients in the confidentiality of their information. The challenge in the age of electronic health information is to maintain trust when electronic medical records are in widespread use.

IV. The HIPAA Privacy Rules

The HIPAA Privacy Rules [FN60] constitute the most significant, extensive, and detailed of several recent attempts by the federal government to protect the privacy of personal information in electronic form. [FN61] The Rules themselves were the product of a circuitous method devised by Congress when enacting HIPAA to break a legislative deadlock over the issue of national health privacy standards. Instead of voting directly on the creation of national privacy standards for health information, Congress directed the Secretary of HHS to submit to Congress recommendations in order to provide guidelines for national health privacy legislation. [FN62] The statute provided that if Congress failed to enact such legislation based on such recommendations by August 21 of 1999, HHS was to be given the authority to promulgate final regulations thereafter. [FN63] When Congress failed to meet ***640** its self-imposed deadline, HHS

promulgated proposed detailed regulations in November of 1999. [FN64] The controversial proposed regulations generated over 52,000 comments. [FN65] Although comments addressed specific aspects of how the rules affected specific industries, a consistent concern expressed by healthcare providers and payers was that the proposed Rules would involve extremely high costs to implement. [FN66] Perhaps because of the potential controversy, the Clinton administration waited until after the election before issuing the final HIPAA Privacy Rules in December of 2000, [FN67] together with a series of other far-reaching and controversial labor and environmental regulations.

On February 28, 2001, with an April 14, 2001 deadline for the Rules to go into effect, the Bush administration's HHS Secretary, Tommy Thompson, reopened the final health privacy regulation for an additional thirty-day public comment period. [FN68] However, on April 12, 2001, the Bush administration announced that the HIPAA Privacy Rules would go into effect largely as originally promulgated by the Clinton administration. [FN69]

***641** On March 27, 2002, the Bush Administration proposed amendments to the HIPAA Privacy Rules, in response to the concerns raised in the second round of comments. [FN70] While the proposed amendments are slightly more pragmatic in spirit than the original Rules, the proposed changes on the whole appear to be relatively minor. The amendments do not make wholesale revisions to the original Rules, and they are largely consistent with the pragmatic and utilitarian spirit of the original rules in balancing the need to protect personal health information against the legitimate reasons for disclosure. The Rules, as amended, still establish effective federal protections for health information with minimal interference on health care treatment, payment and operations.

The Rules face legal challenges. [FN71] There also remains considerable consternation by a health care industry concerned about the significant costs of compliance. [FN72] However, what appears to have emerged over the course of rulemaking by two different political administrations is a bipartisan consensus that a pressing need exists for national standards to protect individually identifiable health information, even if it involves significant costs to the healthcare industry.

Most health plans and healthcare providers that are covered by the Rule have until April 14, 2003 to comply with the requirements of the Rule; [FN73] small health plans have until April 14, 2004. [FN74] The proposed amendments give covered entities an additional year to change their contracts with business associates. [FN75] As the April 14, 2003 compliance date approaches, most health care providers and health plans have resigned themselves to undertaking a significant effort to comply with the new Rules.

A. Overview of the Rules

The HIPAA Privacy Rules were issued in the context of the "Administrative Simplification" provisions of HIPAA, which authorized ***642** national privacy standards in the context of three other closely-related federal regulations: one establishing standardized codes for transactions involving electronic health information, one establishing national security and electronic signature standards for electronic health information, and one establishing national health identifiers. [FN76] The primary purpose of the Administrative Simplification provisions was to adopt national standards to facilitate the electronic exchange of health information to make financial and administrative healthcare transactions more efficient. [FN77] Recognizing that the administrative simplification provisions of HIPAA would increase the dangers of unauthorized disclosure and misuse created by widespread dissemination of electronic health information, Congress directed that the HIPAA Privacy Rules establish detailed nationwide minimum standards for the protection of what it termed "individually identifiable health information." [FN78]

The Rules adopt a pragmatic and utilitarian balance between the need to protect personal health information and the need to disclose personal health information for treatment, payment, public health, research, and other socially beneficial

purposes. The Rules do not pre-empt the patchwork of existing state confidentiality requirements, but they provide a uniform federal floor of protection for personal medical information. [FN79] The Rules also establish fair information practices with respect to personal health information under which individuals are entitled to receive notice of the uses to which their healthcare information is to be put, the right to access their records to verify their accuracy, the right to consent before secondary disclosure may be made for reasons other than the original limited purposes for which the information was collected, the right to an accounting of all such disclosures, and the right to have their personal information maintained securely.

***643** B. Covered Entities Under the Rules

HIPAA limits the application of the proposed rule to (1) health plans, (2) health care clearinghouses, and (3) health care providers. [FN80] A "health care provider" is anyone who furnishes, bills, or is paid for healthcare in the normal course of business. [FN81] This includes doctors, nurses, therapists, and medical technicians. [FN82] It includes hospitals, pharmacists, nursing homes, home health companies, medical equipment providers, and research institutes. [FN83] A "health plan" is any plan that pays for healthcare, whether public or private, including Medicare, Medicaid, other federal and state programs, private health insurance payers, and self-funded plans by employers. [FN84] It also includes Health Maintenance Organizations. [FN85] The term "health plan" excludes, however, insurance under which benefits for medical care are secondary or incidental to other insurance benefits such as property and casualty insurance; disability insurance; liability insurance, including automobile liability; and workers' compensation or similar insurance plans. [FN86] Finally the term "healthcare clearinghouses" includes computer data processing companies, billing companies and reprising companies which process and aggregate computerized health information. [FN87]

Covered entities are required under the Rules to implement compliance programs to ensure that the confidentiality requirements of the Rules are followed. [FN88] These compliance programs involve the establishment of a set of policies to protect the confidentiality of personal health information and a training program for employees in the protection of personal health information. [FN89] The Rules also require the designation of a "privacy official," i.e., an employee responsible for developing and implementing these policies. [FN90]

***644** C. Individually-Identifiable Health Information

The HIPAA Privacy Rules apply to all individually identifiable health information ("IIHI") that is maintained or transmitted "in any form or medium," which would appear to include virtually all written and oral communications in the hands of healthcare providers, insurance payers, and clearinghouses. [FN91] IIHI is defined as information that is created or received by a healthcare provider, health plan, or clearinghouse that relates to the physical or mental health of an individual, as well as the provision of healthcare to an individual or payment for the provision of healthcare to an individual, and that identifies the individual or could be used to identify the individual. [FN92] The Rules allow for the option of de-identifying IIHI prior to its disclosure to third parties. [FN93] However, given the need to identify the patient for most ordinary disclosures of health care information, as well as the uniquely identifying aspects of diagnosis and treatment codes, few ordinary medical providers appear to have engaged in serious attempts to render their medical information anonymous. However, the proposed amendments to the HIPAA Privacy Rules indicate significant efforts to render health information anonymous appear to be taking place in the context of medical research institutions, and the proposed amendments to the Rules relax the requirements for de-identifying IIHI in order to facilitate such efforts. [FN94]

D. Consents and Authorizations

The original Rules created two categories of consents permitting disclosure: "Consents" and "Authorizations."

Healthcare providers "with a direct treatment relationship" were required to obtain a signed consent to use personal health information for treatment, payment, or healthcare operations. [FN95] Such consent forms, however, were largely ritualistic, since the provider was permitted to condition treatment on the execution by a patient of a form consenting to disclosure. In addition, the requirement of signed "consents" runs afoul of the common practice of some providers, such as pharmacists and pharmacies, of using health information for treatment, ***645** payment or health care operations prior to having a face-to-face meeting with the patient. The proposed amendments drop the requirement that health care providers obtain signed "consents" from their patients, recognizing both the ritualistic and impractical aspects of such a requirement. [FN96] Under the proposed amendments, health care providers may but are not required to utilize such a consent form. [FN97] Thus, under the Rules as amended, whether or not a consent form is obtained, providers may disclose personal health information for purposes of treatment, payment or health care operations. [FN98]

A health care provider may continue to disclose personal health information without the authorization or consent of a patient for purposes of public health reporting; to report instances of child abuse and neglect and other forms of domestic violence; for health oversight activities; for purposes of judicial and administrative proceedings; for law enforcement purposes; to avert a serious threat to life and safety; to identify deceased persons; and where otherwise required by state or federal law. [FN99] The amendments to the Rules do not change the required disclosures that take place "as required by law." [FN100] Such disclosures are largely identical with those discussed in this Article under the heading of Public Health and Safety. [FN101] Thus, however controversial many state mandated disclosures for public health and safety may be, the HIPAA Privacy Rules do not alter the balance between individual privacy and public health and safety reached by various state and federal lawmakers and courts in requiring such disclosures. For purposes of payment, treatment and health oversight, as well as for purposes of public health and safety, the HIPAA Privacy Rules largely leave the former system of health care disclosures unchanged.

For most other disclosures, with the exception of research, a formal signed authorization must be obtained from the individual who is the subject of the information. [FN102] The requirement of a formal signed authorization represents a departure from the status quo before the Rules. The proposed amendments to the Rules simplify the requirements for obtaining an ***646** authorization, but leave the basic concept intact. [FN103] An authorization is different from a patient "consent" and is much more difficult to obtain. It requires a detailed explanation to the individual of the proposed use or disclosure. [FN104] If the HIPAA Privacy Rules do not expressly permit or require use or disclosure of personal health information without individual authorization, a covered entity must obtain a signed authorization from the individual. [FN105] The Rules require individual authorization for use and disclosure of psychotherapy notes in most circumstances. [FN106] Finally, a covered entity may not condition an individual's treatment, payment, enrollment, or eligibility on the provision of an authorization. [FN107] The patient also retains the right later to revoke the authorization. [FN108]

The Rules' strict requirements with respect to "authorization" forms are intended to address abuses of broad consent or authorization forms. Such broad consent forms had become a standard part of visits to some healthcare providers. While most reputable healthcare providers limited the language on such forms to disclosures for treatment and payment, unscrupulous providers and insurance companies had sometimes used the broadly drafted forms to legitimate disclosures of medical information for purposes entirely unrelated to treatment, payment or health oversight decisions. [FN109] Since the ability of patients to receive the care or service could be conditioned on their signing the broad consent form precisely when they were most vulnerable, such forms lacked any meaningful notion of consent. These broadly drafted release forms were aptly called by Professor Turkington "the black hole" of confidentiality. [FN110] The Rules largely have eliminated these abusive practices. The overall effect is that other than for the purposes of treatment, payment, health oversight, public health and safety, and research, the Rules prohibit the flow of identifiable information for any additional purposes unless specifically and voluntarily authorized by the subject of the information.

Disclosures for purposes of marketing are listed among the disclosures for which the proposed amended Rules expressly require an authorization ***647** form to be signed by the patient. [FN111] Thus, covered entities may not disclose protected health information to third parties for purposes of marketing without the express permission of the patient. [FN112] However, the amended Rules narrow the definition of marketing to exclude the marketing of goods and services provided by the covered entity, permitting health care providers to market their own goods and services to their patients.

With certain limited exceptions, discussed below, the HIPAA Privacy Rules require an authorization to be obtained by researchers. [FN113] The proposed amendments to the Rules slightly alter the conditions under which the authorization of the subject of the research must be obtained, but they do not fundamentally change the general requirement. [FN114] In this respect, the Rules place all covered entities conducting research, whether they be federally funded or privately funded, under the same requirements with respect to the confidentiality of any human subjects of the research. Under all circumstances, IRB's will be required to oversee the authorization forms obtained by both public and private researchers. [FN115] In the event that the authorization of the subject of the research cannot be practically obtained, the IRB must find that the use or disclosure of protected information involves no more than a minimal risk to the privacy of the individuals and that the research could not be practically conducted if the researchers were required to obtain such authorizations. [FN116] In addition to placing all researchers, whether public or private, under the control of an IRB, the HIPAA Privacy Rules establish minimum privacy requirements and require coordination with privacy officers that had not previously been required even of federally funded researchers. [FN117]

E. Minimum Necessary Disclosure Standard

Other than for purposes of treatment, the regulations provide that most uses, disclosures, and requests for disclosures of personal health information are subject to the "minimum necessary standard" under which a covered entity "must make reasonable efforts to limit protected health information to ***648** the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [FN118] The Rules permit covered entities flexibility in the determination of what constitutes "reasonable efforts." [FN119] The proposed amendments to the Rules also make it clear that this provision allows for a broad range of reasonableness as to what "minimum necessary" means for each provider. [FN120] As described in the proposed amendments to the Rules, the minimum necessary requirement is a reasonableness standard--requiring health care providers to balance the costs and burden to covered entities in implementing the standard consistent with the professional judgment of the health care providers. [FN121] The proposed amendments to the Rules acknowledge the "slack" in confidentiality that accompanies what is sometimes the hectic provision of health care in a hospital setting discussed above. [FN122] The Rules permit a health care provider to employ a strong dose of pragmatism in interpreting the minimum necessary requirement. [FN123] What the minimum necessary requirements in the Rules do require, however, is for the health care provider to exercise reasonable care with respect to questions of confidentiality in the day-to-day practice of medicine. The requirement of reasonable care was also imposed on health care providers under the existing state law of confidentiality. Thus, the Rules largely codify under federal law the pragmatic approach to confidentiality previously in place under state law. The Rules, however, have forced the medical industry to focus on its existing duty of reasonable care in the context of a new world of networked computer systems.

F. Fair Information Practices

The most significant change in the Rules concerns the creation of a set of fair information practices with respect to personal health information. In the United States, the concept of fair information practices was developed in the late 1960s and early 1970s out of concerns about the implications of widespread conglomerations of personal information in computerized ***649** databases. [FN124] In 1973, a path-breaking report by the Department of Health, Education, and Welfare entitled Records, Computers and the Rights of Citizens [fn125] (THE "HEW Report") ADDRESSed certain fundamental principles involved with the use of electronic information to collect, access, and store information about

individuals. To address these concerns, the HEW Report articulated a set of general principles entitled a "Code of Fair Information Practices." [FN126] This Code set forth general principles under which individuals would be entitled to receive some form of notice of the uses to which their healthcare information is to be put, a right to access their records to verify their accuracy, the right to consent before secondary disclosure may be made for reasons other than the original limited purposes for which the information was collected, the right to an accounting of all such disclosures, and the right to have personal information maintained securely. [FN127] Various aspects of fair information practices have been incorporated into numerous federal statutes, including the Federal Privacy Act of 1974, [fn128] THE FAMILY EDUcatioNal riGHts and privAcy act of 1974, [fn129] AND the Video Privacy Protection Act of 1988, [FN130] as well as many similar state statutory privacy ***650** protection schemes. In Europe, the European Community has adopted similar fair information practices in the form of the Privacy Directive. [FN131]

The HIPAA Privacy Rules incorporate a full set of the requirements of fair information practices. Patients are entitled to receive a notice of the institution's privacy policies allowing them to know who is using their health information and how it is being used. [FN132] Patients have the right to inspect and copy their own personal health information. [FN133] They have the right to request amendments of erroneous or incomplete information. [FN134] They have the right to obtain an accounting of any disclosures of their information for any purposes other than treatment and payment. [FN135] They have the right to file complaints if they believe the covered entity has not followed its privacy policies. [FN136] The Rules require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure, and covered entities must implement safeguards to protect health information from intentional or accidental misuse. [FN137]

G. Business Associates

As we have seen, the HIPAA Privacy Rules apply only to covered entities. They do not directly cover what the Rules call "Business Associates" of providers and plans. Business associates constitute those businesses and individuals who provide services or a product that involves the transfer of individually identifiable medical information. [FN138] Business associates include third-party administrators, some billing firms, pharmacy benefit management companies, disease management firms, companies that provide utilization review, companies that provide management or quality assurance services, and companies that perform data processing operations for health plans and healthcare providers. [FN139] Business associates also ***651** include lawyers and accountants who work for healthcare providers and health plans. [FN140]

Recognizing that failure to address the responsibilities of business associates within the system of disclosures of personal health information would vitiate the effectiveness of the Rules themselves, the drafters of the Rules began with a simple fact: that virtually all access by business associates to personal health information originates with healthcare providers and payers. As such, the Rules provide that while only covered entities are subject to the Rules, covered entities may not provide information to business associates without a written contract placing the business associate under the same requirements to safeguard health information as the covered entities. [FN141] Since all personal health information derives ultimately from healthcare providers who are in turn under a duty of confidentiality to the individual patient, the Rules thus put business associates under a contractual obligation that makes them agents of the covered entities with respect to the business associates' use of personal health information with the same duties of confidentiality with respect to the personal health information as the covered entity. The requirement of the existence of a contract between the covered entity and the business associate also ensures that the legal responsibility of the business associate with respect to confidentiality is properly documented. [FN142]

H. Enforcement of the Rules

The Rules are enforced through criminal and administrative penalties. Administratively, the HHS Secretary has the authority to impose civil monetary penalties against covered entities that fail to comply with the requirements of the Rule. [FN143] The fines the secretary is permitted to levy are limited to $25,000 for each calendar year for each provision that is violated. [FN144] As a matter of criminal law, the HIPAA statute provides much stronger criminal penalties for wrongful disclosures of protected health information, including imprisonment for up to ten years and substantial fines if the offense is committed under false pretenses, or with intent to sell the ***652** information or reap other personal gain. [FN145] These sanctions, however, apply only to covered entities. [FN146] For instance, criminal or administrative remedies do not appear to apply to business associates that misuse personal health information. While covered entities must take "reasonable steps" to ensure their business associates are in compliance with their "business associate contracts," the proposed rules make the covered entities responsible for ensuring the compliance of their business associates. [FN147] The failure of the Rules to create direct sanctions against "business associates" who engage in misconduct represents an important shortcoming in the regulatory framework under HIPAA.

V. Breach of Confidentiality and its Implications

A. Breach of Confidentiality Under the Common Law

The Preamble to the final HIPAA Privacy Rules explains that the chief reason for the need of federal protections for personal health information is the lack of significant protections for the privacy of medical records under state common law and statutes. [FN148] In fact, in the following discussion, this Article argues that not only does the common law provide relatively strong protections, but effectively may cure the two principal weaknesses of the Rules--their failure to create a private right of action against entities that misuse personal information, and the lack of any sanctions for business associates of covered entities which misuse personal information. The drafters of the Rules themselves call for the enactment of a federal "private cause of action" to enforce the privacy of healthcare records and expanded authority to address the problem of "downstream" liability for wrongful disclosures. [FN149] The failure of the Rules appears to leave an important gap in the enforcement structure. This Article argues that the Rules will interact with sate common law doctrines to fill in this gap.

The drafters of the Rules are correct in one respect. The common law torts for invasion of privacy do not offer significant protection in the context ***653** of personal health information. [FN150] Most courts have found that to establish a claim for public disclosure of private records, the plaintiff must show a widespread disclosure to the public--something that will not occur in most cases involving the release of health information. [FN151] Another restriction of the public disclosure tort is that the requirement that the release of information be to someone without a legitimate interest in the information. [FN152] Of course, it is precisely those with a legitimate interest in personal health information, such as employers, for whom the disclosure of health information is most problematic. The disclosure of health information to strangers, who have no interest in the information at all, often poses a marginal threat or no threat at all. Finally, and most importantly, to recover under an invasion of privacy theory, the plaintiff must typically establish that the disclosure was intentional, [FN153] while most disclosures of health information happen by accident or through negligence.

Because both the torts of invasion of privacy and breach of confidentiality are aimed a protecting information, it is easy to assume that the two torts serve fundamentally the same purposes. This is a mistake. Philosophically, privacy is a right with respect to personal information based on notions of individual dignity and respect. Claims for invasion of privacy ***654** do not depend on the existence of a relationship of trust between the defendant and the injured party, but are based on the misuse of the personal information due to the sensitive and private nature of the information. On the other hand, breach of confidentiality represents an injury to a relationship of trust between the injured person and the person who has misused the information, and the tort has as its purpose the need to maintain the integrity of that relationship. Because of the deep and profound differences between the concept of privacy and the concept of confidentiality, it does not follow

that the failure of the invasion of privacy torts to address improper disclosures of health information implies the failure of breach of confidentiality theories as well. If invasion of privacy torts do not protect personal health information effectively, it may be that they were never designed to do so. On the other hand, the tort of breach of confidentiality originated in the context of healthcare and was specifically designed to consider the problems of protecting health information. [FN154]

The vast majority of states recognize that an actionable tort lies for a physician's breach of the duty to maintain the confidences of his or her patient in the absence of a compelling public interest or other justification for the disclosure. [FN155] Either as a matter of statutory law or as a matter of common law, courts have not shied away from finding a public policy in favor of a patient's right to confidentiality and have allowed plaintiffs to recover for improper disclosure of their personal health information. Courts have found indications of a public policy to protect the confidentiality of personal health information in the possession of physicians in statutes that ***655** create a testimonial privilege with respect to confidential communications between a patient and a physician, and in licensing statutes that authorize the suspension or revocation of a license to practice medicine if a doctor divulges a professional secret without authorization. [FN156] These indications have also been found under common law principles of trust, the Hippocratic Oath, and principles of medical ethics that prohibit the revelation of patient confidences. [FN157]

One of the earliest cases discussing the liability of a physician for disclosure of patient information is Simonsen v. Swenson, [FN158] a case in which a physician had treated a patient while the patient was staying in a hotel. [FN159] The patient filed suit for breach of confidentiality after the doctor disclosed to the hotel operator that the patient had a "contagious disease" and advised her to be careful to disinfect the patient's bed clothing and wash her hands in alcohol afterwards. [FN160] The court reviewed both the ethical standards applying to physicians and evidentiary statutes creating a privilege for such communications to infer that breach of confidentiality was in fact an actionable claim. [FN161] However, under the circumstances of the case, the court found that the disclosure was privileged as necessary to prevent the spread of disease, and found no violation of the physician's duty. [FN162]

In subsequent cases finding a common law tort of breach of confidentiality, courts generally have relied on statutes and ethical rules, which, while not providing an individual cause of action for their violation, are used to establish the standard of care that allegedly has been violated. In Horne v. Patton, [FN163] Horne's physician disclosed Horne's medical information to his employer, contrary to Horne's express instructions. [FN164] Horne alleged that the doctor-patient relationship was a confidential relationship that created a fiduciary duty by the doctor, that the unauthorized release of information breached the fiduciary duty, and further, that it ***656** violated the Hippocratic Oath, constituting unprofessional conduct. [FN165] The Supreme Court of Alabama held there was a confidential relationship between a physician and a patient that imposed a duty upon the physician not to disclose information concerning the patient obtained in the course of treatment. [FN166] The court noted that, although the state had not enacted the physician-patient testimonial privilege, this did not control the issue of liability of a physician for unauthorized, extra-judicial disclosures of such information. [FN167] The court stated it is "important that patients seeking medical attention be able to freely divulge information about themselves to their attending physician without fear that the information so revealed will be frivolously disclosed. . . ." [FN168]

Likewise, in Hague v. Williams, [FN169] in determining that New Jersey recognized the breach of confidentiality tort although finding against the plaintiff, the Supreme Court of New Jersey stated that, ordinarily, a physician receives information relating to a patient's health in a confidential capacity and should not disclose such information without the patient's consent, except where the public interest or the private interest of the patient so demands. [FN170] The court observed that it was not concerned with the physician-patient privilege because "it deals with testimony in a judicial proceeding." [FN171] The court explained the importance of the physician-patient duty of confidentiality in the following passage: "A patient should be entitled to freely disclose his symptoms and condition to his doctor in order to receive

proper treatment without fear that those facts may become public property. Only thus can the purpose of the relationship be fulfilled." [FN172] Similarly, in Humphers v. First Interstate Bank of Oregon, [FN173] the Supreme Court of Oregon held that the actionable wrong was the breach of the duty arising from a confidential relationship. [FN174] It noted that a statute providing for the disciplining of a physician who divulges a professional secret "only establishes the duty of secrecy in the medical relationship." [FN175] The court did ***657** not ground its decision on the statute, but upon the common law duty that was breached by the defendant. [FN176]

As Alan B. Vickery writes:

(T)he duty of confidentiality, where it exists, generally arises out of broadly applicable societal norms and public policy concerning the kind of relationship at issue. It does not arise out of specific agreement or particularized circumstances. Moreover, the object of the law when this duty is violated is compensation for the resulting injuries, not fulfillment of expectation. Therefore, liability should be grounded in tort law. [FN177]

Courts have sometimes also addressed claims for improper disclosure of patients' medical records on the alternative theory of invasion of privacy. [FN178] While it is accurate to describe a breach of confidentiality as a breach of an implied term of a contract, when invasion of privacy concepts are considered in the context of breach of confidentiality decisions, there is a danger that two different torts are becoming confused.

First, in the tort of breach of confidentiality, the unauthorized revelation of confidential medical information is protected without regard to the degree to which the information has been published to the general public. [FN179] Both the invasion of privacy tort and the breach of confidentiality tort rest on wrongful disclosure of information, but the disclosure involved in an invasion of privacy tort consists of the public disclosure of private facts about the plaintiff. [FN180] Where the information disclosed is received in confidence, as we have seen in the general discussion above, the greatest injury from the breach of confidence of a physician may result from disclosure to a single person such as a spouse, or to an employer. [FN181]

Second, to establish a claim for invasion of privacy, the disclosure must be highly offensive to a reasonable person. [FN182] In a breach of confidence ***658** case, the information is protected without regard to the degree of its offensiveness. [FN183] If the a breach of confidence by a physician causes subjective embarrassment to the patient, even if a reasonable person might not find the disclosure offensive, the physician can still be liable. [FN184]

Third, while a breach of confidentiality case must involve an intentional disclosure, [FN185] a breach of confidentiality by a physician can be unintentional or accidental. [FN186] Breach of confidentiality can be established merely upon a showing of failure to take reasonable care to protect the sensitive health information. [FN187]

Fourth, there is no defense to an action for breach of confidentiality that the facts disclosed are of public interest. [FN188] In the context of claims alleging invasion of privacy by public disclosure of private facts, Courts tend to narrowly construe the zone of proscribed conduct in order to prevent hindrance of public expression, either under the common law itself, or as a matter of constitutional law to protect freedom of expression. [FN189]

The invasion of privacy tort protects the right of an individual to "be left alone." It is the right to exercise control over the disclosure of information that is "private" and the right extends to any member of the public who may come into possession of that information. This broad assertion of control over information, qua information, contrasts sharply with a right to confidentiality, which "exists only against a specific person, who, by virtue of his relationship to the confider, has notice of the duty to preserve the secrecy of clearly identifiable information." [FN190]

Confidential information presupposes as a predicate an initial disclosure of information to another person.

Confidentiality, thus, in its essence, is a condition placed on information based on the nature of the relationship between the parties in which the information is exchanged--the doctor and the patient, the lawyer and the client, the priest and the penitent. No matter how sensitive this information may be, without such a relationship, the can be no confidentiality.

***659** B. Justified Disclosures Not a Breach of Confidentiality

When health information is disclosed in a manner that causes harm to the patient there is a presumptive cause of action for breach of confidentiality. However, there is a broad range of contexts in which the disclosure of health information by a medical professional is justified. In these instances, under the case law, a disclosure is not actionable, even if it is not made with the consent of the patient. For instance, as we have seen, a physician does not typically need to obtain the consent of a patient in order to consult with another physician, such as a specialist, about the health of the patient. We have already examined Simonsen v. Swenson, [FN191] the very earliest American common law case involving a claim for breach of confidentiality. In that case, the Court found the physician's disclosure was justified and privileged. [FN192] Likewise, state statutes placing an affirmative duty on physicians to disclose certain types of health conditions for public health reasons also expressly or impliedly provide a grant of immunity from liability for breach of confidentiality for such disclosures. [FN193]

In general, the breach of confidentiality theory allocates liability using a pragmatic balancing test, permitting disclosures to take place when the need to disclose the information outweighs the interests in keeping the information confidential. For instance, public policy requires that where it is reasonably necessary to protect the interest of the patient or others, a physician may disclose confidential patient information without incurring liability for breach of confidentiality. [FN194]

***660** If the entities to which such information is disclosed are under a legally enforceable duty of confidentiality similar to that of the physician, the balancing of costs and benefits tends to be more favorable to disclosure. [FN195] As in the case of statutes and regulations that require the sharing of personal medical information for public health purposes, fraud investigations, and other socially beneficial reasons, [FN196] these required disclosures also create a "chain of trust"--that is, persons who come into possession of individual health information are themselves under duties of confidentiality mandated by law. [FN197] Thus, the breach of confidentiality tort evidences a pragmatic and utilitarian balancing which permits disclosures of medical information when these disclosures serve a legitimate purpose, when the public benefit of disclosure or danger from non-disclosure outweighs the harm inflicted on the relationship of trust between patient and physician, and there is maintained a "chain of trust" preventing further improper disclosures which may harm the patient.

An example of such balancing under the common law is the case of Estate of Behringer v. Medical Center at Princeton. [FN198] The case involved a physician at a hospital whose positive test for HIV was disclosed to fellow personnel at the hospital where he worked and to his patients. [FN199] In finding liability for breach of confidentiality, the court noted that the disclosure of confidential information by the hospital did not have to be intentional, but sounded in common law negligence for failing to take reasonable measures to protect patient medical records against unauthorized access and use by members of the staff. [FN200] What the court rightly focused on was not an absolute duty to protect against disclosures of confidential medical information, but the fact that while the hospital's procedures may have been sufficient to protect against breaches of confidentiality for members of the general public using the hospital, it was not sufficient to protect from disclosures of information about hospital staff. [FN201] The tolerance of inadvertent disclosures of medical information among the staff proved precisely the undoing of the hospital when the information most needed to be protected from the hospital staff themselves. [FN202] The court held that the ***661** design and management of a health records system is a duty that requires a medical provider to balance the possible harm from unauthorized disclosure against the cost of reducing the risk of disclosure. [FN203]

As the Behringer case illustrates, the common law effectively regulates use. Disclosure is actionable only if it causes harm. Confidential medical information is unlikely to have much relevance or significance to a stranger, so disclosure to a stranger tends to cause less harm than disclosure to friends, relations, customers, clients, and other non-strangers. In Behringer a system was implemented by the hospital to prevent misuse of information, but was designed to protect information from outsiders. When the subject of the AIDS test was a doctor at the hospital, the system failed to protect against the destructive consequences of the disclosure to the doctor's business colleagues, friends, and patients. The court found the harm caused by this disclosure to have been foreseeable, and found liability.

Most disclosures of medical information are not reasonably foreseeable to cause harm. For instance, unauthorized disclosures of confidential medical information may take place in the processing of medical claims and payments, but the strangers performing data processing services are not in a position to use the confidential medical information in a manner that harms the subject of that information. The question asked by the court in Behringer is whether the hospital's procedures for shielding against wrongful disclosure of medical information were reasonable--appropriately balancing the potential harms from disclosure against the cost to the hospital.

C. Downstream Third Party Liability for Breach of Confidentiality

As the Warren and Brandeis law review article noted, the breach of confidence tort requires the existence of a relationship of trust and is ineffective when a relationship of trust cannot be established. [FN204] Because of the necessity of establishing a relationship of trust, well-respected scholars have argued forcefully that breach of confidentiality theories are inadequate to protect the privacy of medical records in an age where, as we have seen, electronic medical records are so widely disbursed in the health care industry. [FN205] Lawrence O. Gostin writes as follows:

***662** Our past thinking assumed a paper record created and protected by the provider. We must now envision a paptient-based record that anyone in the system can call up on a screen. Because location has less meaning in an electronic world, protecting privacy requires attaching protection to the health record itself, rather than to the institution that generates it.... [FN206]

Gostin is correct that under traditional breach of confidentiality theory, courts have expressed the tort as existing only between those in a direct relationship with each other. [FN207] As such, it would seem to be difficult to find liable under breach of confidentiality theories third parties who are downstream in the information flow. For instance, if confidential medical information is passed from a physician to an insurer, does the insurer holding the medical information also have a duty to maintain the confidentiality of the information? When cases have directly presented claims regarding misuse of personal health information by "downstream" entities in the health information flow, the answer which has been provided by at least some common law courts is yes. For instance, breach of confidentiality can be committed not only by a provider in a direct relationship with a patient, but also by downstream user of that information such as an insurance company, which lacks a direct relationship of confidentiality with the patient.

In Hammonds v. Aetna Casualty & Surety Co., [FN208] Hammonds was a plaintiff in a suit against an insurance company that was also Hammond's treating physician's malpractice insurer. [FN209] The insurance company was alleged to have obtained from the physician Hammonds' confidential medical records under the pretext that Hammonds was contemplating a malpractice suit against the physician. [FN210] Hammonds brought suit against the insurance company for inducing the physician to divulge confidential information gained through a physician-patient relationship. [FN211] The physician was also a nominal defendant, but the complaint only accused the physician of "misfeasance predicated on misinformation" and directed its ***663** plea for redress solely against the insurance company. [FN212] The court, in a prior proceeding, found that "one who induces a physician's treachery may also be held liable for damages." [FN213] In denying defendant's motion for reconsideration, the court held that "when one induces a doctor to divulge confidential

information in violation of that doctor's legal responsibility to his patient, the third party may also be held liable in damages to the plaintiff." [FN214] The courts in Ohio do not restrict this holding to insurance carriers that obtain confidential information from physicians through the use of pretexts. [FN215]

In Alberts v. Devine, [FN216] two clerical superiors of a Methodist minister obtained confidential treatment information from the plaintiff's psychiatrist and used this information to the detriment of the plaintiff in his employment decisions. [FN217] In finding liability not only against the psychiatrist but also against the third parties to whom disclosure was made, the Supreme Judicial Court of Massachusetts outlined three elements that must be present in order to establish liability for inducing a physician to breach his duty of confidentiality:

To establish liability the plaintiff must prove that: (1) the defendant knew or reasonably should have known of the existence of the physician-patient relationship; (2) the defendant intended to induce the physician to disclose information about the patient or the defendant reasonably should have anticipated that his actions would induce the physician to disclose such information; and (3) the defendant did not reasonably believe that the physician could disclose that information to the defendant without violating the duty of confidentiality that the physician owed the patient. [FN218]

Alberts was followed in Morris v. Consolidation Coal Co. [FN219] In that case, the Supreme Court of Appeals of West Virginia found liability not only against the physician, but the third party as well. [FN220] Morris also involved a disclosure of confidential medical information by a physician to an employer ***664** in the context of a workmen's compensation dispute. [FN221] The court addressed the question of whether a patient has a cause of action against a third party who induces the physician to breach his fiduciary relationship by disclosing confidential information, answering the question in the affirmative. [FN222]

Very recently, in the case of Biddle v. Warren General Hospital, [FN223] the Ohio Supreme Court held that in addition to a hospital's liability for breach of confidentiality, the law firm representing the hospital could also be held liable for inducing the hospital to breach patient confidentiality. [FN224] The hospital disclosed patient medical information to the law firm in order to allow the law firm to research the eligibility of the patients for coverage under Supplemental Security Insurance Disability benefits (SSI). [FN225] If the patients were found eligible for SSI, Medicare would pay their hospital bills. [FN226] It was expected that the law firm would provided legal representation to some of these patients in attempting to get SSI benefits. [FN227] While the court recognized the need in some contexts for an attorney representing a healthcare provider to review personal medical information, permitting the law firm to review virtually every patient file in the hospital was found not to be reasonable. [FN228] In addition, the court was clearly troubled by the multiple hats the law firm appeared to be wearing. It was not clear whether the law firm was accessing the patient records for the benefit of the hospital, or so that the law firm could attract new clients. [FN229]

The general rule developing from the line of cases discussed above appears to be that a patient has a cause of action against a third party who induces a physician to breach his fiduciary relationship if the following elements are met: (1) the third party knew or reasonably should have known of the existence of the physician-patient relationship; (2) the third party intended to induce the physician to wrongfully disclose information about the patient, or the third party should have reasonably anticipated that his actions would induce the physician to wrongfully disclose such information; (3) the third party did not reasonably believe that the physician could disclose that information to the third party without violating the duty of ***665** confidentiality that the physician owed the patient; and (4) the physician wrongfully divulges confidential information to the third party.

D. Private Causes of Action for Breach of Confidentiality Under the HIPAA Privacy Rules

As we have seen, the HIPAA Privacy Rules do not create a private right of action or any other mechanism for individuals to enforce their rights under the Rules. The Secretary's Recommendations to Congress on HIPAA included

proposal that Congress there be a private right of action. [FN230] However, Congress provided that the scope of the government's ability to bring enforcement proceedings under the Rules is limited to covered entities, and did not provide for a private cause of action for individuals to enforce their rights under the Rules. The question thus arises how the standard of protection of personal health information and the fair information practices implemented in the Rules will interact with the common law action for breach of confidentiality.

While this question is somewhat speculative, several general observations can be made regarding this interaction. First, because the Rules preempt state confidentiality laws that provide a lower level of protection than the Rules, the Rules establish a clearly delineated federal floor of protection for confidential health information. Will this become the floor establishing the minimum standards in a common law action for breach of confidentiality? This question breaks into two questions. The first question, whether the HIPAA Rules will be read as creating a private federal cause of action, would appear to be answered in the negative. The second question, whether the Rules will be adopted by state courts as a minimum standard in common law breach of confidentiality claims, would appear to be answered in the affirmative.

In Cort v. Ash, [FN231] the Supreme Court enunciated the following four-part test for implying a private cause of action for the violation of a federal statute:

***666** First, is the plaintiff "one of the class for whose especial benefit the statute was enacted,"--that is, does the statute create a federal right in favor of the plaintiff? Second, is there any indication of legislative intent, explicit or implicit, either to create such a remedy or to deny one? Third, is it consistent with the underlying purposes of the legislative scheme to imply such a remedy for the plaintiff? And finally, is the cause of action one traditionally relegated to state law, in an area basically the concern of the (s)tates, so that it would be inappropriate to infer a cause of action based solely on federal law? [FN232]

In more recent cases the Supreme Court has looked almost exclusively to congressional intent--the Cort criteria being treated as indicia of that intent. [FN233] Since deciding Cort, the Court has become increasingly reluctant to imply new private causes of action for damages. [FN234] In the Court's most recent case, Gonzaga University v. Doe, [FN235] it addressed the question whether the non-disclosure provisions of the Family Education Rights and Privacy Act ("FERPA") [FN236] created a private cause of action for their violation. FERPA prohibits educational institutions that receive federal funds from releasing the educational records of their students to unauthorized persons. [FN237] The Court held that for Congress to create new rights enforceable by a private cause of action, it must do so in clear and unambiguous terms. [FN238] Where, as in FERPA, there was an alternative enforcement mechanism established--in FERPA, the revocation of federal funding--the Court held no private cause of action could be inferred. [FN239]

Returning to the question of whether an implied cause of action exists for violation of the HIPAA Privacy Rules, given the provision by Congress of both criminal and administrative remedies for violations of the HIPAA Privacy Rules, it seems unlikely that courts would imply a private federal cause of action for the violation of the Rules. However, it does not follow ***667** that the Rules will not become the basis of a private cause of action under state law.

The defendant in most negligence per se cases already owes the plaintiff a pre-existing common law duty to act as a reasonably prudent person, so that the statute's role is merely to define more precisely what conduct breaches that duty. For example, the standard negligence per se case involves violations of traffic statutes by drivers. These are actors who already owe a common law duty to exercise reasonable care toward others on the road or track. When a statute criminalizes conduct that is also governed by a common law duty, as in the case of a traffic regulation, applying negligence per se causes no great change in the law because violating the statutory standard of conduct would usually also be negligence under a common law reasonableness standard. [FN240] While recognizing a new, purely statutory duty "can have an extreme effect upon the common law of negligence" when it allows a cause of action where the common law would not, [FN241] in the case of the HIPAA Privacy Rules, applying the federal standards in state

common law tort suits does not bring into existence a new type of tort liability, but merely clarifies the standard that applies to a previously existing duty. When the statute or regulation on which civil liability is based corresponds exactly to a previously existing common law duty, the use of that statute or regulation to specify the scope and extent of the common law duty is a standard and unproblematic exercise of traditional tort doctrines. [FN242] The addition of a federal regulatory scheme does not change this analysis. For instance, even when courts determine a federal regulation or statute has entirely pre-empted a field of the law, they have still concluded, "that the traditional state and territorial law remedies continue to exist for violation of those standards." [FN243] If a court declines to imply a federal right of action, "the federal statutes may create a standard of conduct ***668** that would give rise to an action, for common-law negligence." [FN244] A state court is " 'free to look to the provisions of a federal statute for guidance in applying its longstanding common( )law remedies' unless Congress has prohibited the state from looking to the statute's provisions as a standard in determining whether there has been a common( )law breach." [FN245] Given the express intention of Congress and the drafters of the Rules not to pre-empt any state laws granting greater rights to privacy in personal health information, [fn246] IT FOLLOWS THAt, especially when the federal hipaa privacy rULES establish a higher standard than that provided under the law of a state, the Rules will be adopted by state courts as specifying the requisite duties of confidentiality owed under state law.

Since a violation of the HIPAA Privacy Rules by a healthcare provider that results in damage to a patient is one and the same thing as a breach of the covered entity's duty of confidentiality to the patient under pre-existing state law, it would seem that the minimum standards of confidentiality set forth in the Rules will inevitably be adopted as the minimum standards for purposes of establishing liability when courts entertain suits for common law breach of confidentiality in instances where personal health information is misused.

1. Liability for Disclosure to Employers

The advent of the Employee Retirement Income Security Act of 1976 (ERISA) [FN247] led to the replacement of private independent health insurance carriers by health plans funded by employers as the principal financing vehicle for the payment of private healthcare. [FN248] The employer, as the plan sponsor, is responsible for payment of the health claims; the insurance company is usually charged only with processing the claims according to the terms of the plan document. [FN249] As plan administrator, an employer is able to review all claims paid by the administration company, which necessarily ***669** includes specific information concerning diagnosis and treatment. Employers often maintain a company file of all medical insurance claims for each employee at the company. At times, employers with access to such information have used this information in ways that had a detrimental impact on an employee's employment. Although access by an employer to such detailed medical information is extremely problematic, most state confidentiality standards applicable to the improper use and disclosure of personal health information are pre-empted by ERISA, which lacks any equivalent provisions for the protection of patient confidentiality and privacy. [FN250]

The advent of the HIPAA Privacy Rules represents a significant change in the standards applicable to the use of employee medical information by employers. Most players within the healthcare industry, whether they are healthcare providers or insurance company payers, have over the years developed a culture in which there is a relatively high degree of respect for the confidentiality of medical records. The HIPAA Privacy Rules are largely consistent with the underlying duties of confidentiality the health care industry is familiar with, and the adjustments which health care industry will be required to make as a result of the Rules may involve a significant expense, but will not fundamentally alter ordinary practices and expectations in the industry. On the other hand, most employers maintaining self-funded health plans have never developed a similar culture of respect for health information confidentiality. While some large employers such as IBM have for many years maintained internal controls on access to employee health information, most employers who sponsor self-funded employee benefit plans which pay health claims will be required to initiate significant changes in their practices and culture in order to comply with the Rules. More troubling, few employers sponsoring self-funded

employee benefit health plans appear to even be aware of the upcoming compliance date for the Rules. In part this may be explained by the fact that under the Rules, the "ERISA plan" and not the plan sponsor is actually the covered entity. [FN251] However, the legal distinction between employer and plan is often lost as a practical matter when the trustees of the plan are usually senior managers of the employer. HIPAA will put an end to the previous practice of employers accessing personal health information from health plans and using that ***670** information for purposes of making employment decisions. [FN252] Under the Rules, health plans maintained by employers are covered entities with similar duties to protect the confidentiality of personal health information. The Rules permit disclosure of personal health information from the plan to the plan sponsor only if one of four requirements is met.

(1) The covered entity is a healthcare provider that is a member of the workforce of the employer; or provides medical care to the individual at the request of the employer to conduct workplace medical surveillance, or to evaluate whether the individual has a work-related illness or injury;
(2) The personal health information disclosed concerns findings related to work-related illness or injury;
(3) The employer needs the findings to comply with obligations to record such illness or injury, or to perform surveillance under various federal or state safety laws; or

(4) The provider gives written notice to the individual that the personal health information will be disclosed to the employer by copy to the individual at the time the healthcare is provided, or if the healthcare is provided at the work site, by posting the notice in a prominent place at that location. [FN253]

Thus, except for these limited instances, the Rules would appear to end the practice by employers of surreptitiously accessing personal health information from self-funded health plans and using this information to make employment decisions. Doctors, hospitals, and healthcare providers have long faced common law liability for breach of confidentiality. However, for employers with self-funded health plans, who for the first time have duties of confidentiality as covered entities and face criminal and administrative penalties, the change created by the HIPAA Rules is likely to be quite abrupt.

Even more significant than potential criminal and administrative enforcement proceedings against such employers is the potential liability under state common law breach of confidentiality theories. Such theories are very likely to be pursued in the context of contentious employment litigation when it appears that employers have accessed employee medical information ***671** outside of the context of the Rules. The success of such actions is likely to be determined by the question of whether employers have duties of confidentiality under state common law. We have reviewed the developing trend in the common law finding employers liable under an "inducement to breach of confidentiality," illustrated in such cases as Alberts v. Devine [FN254] and Morris v. Consolidation Coal Co. [FN255] It is noteworthy that the employers in these cases did not have a pre-existing duty, but their duty was derivative of that of the physician. Because under the HIPAA Privacy Rules the self-funded health plan itself is a covered entity, the traditional access by an employer to personal health information contained in payment records of the plan without a signed authorization from the employee constitutes a direct violation of the Rules. Thus, a court would not have to adopt "downstream" theories to find liability. An employer may argue that because the plan is the covered entity, liability for breach of confidentiality is limited to the plan and cannot be extended to the employer. The practical reality is that this is a distinction without a difference. The management of the employer and the management of the plan are usually the same individuals, and a judgment against the plan would nearly always have to be satisfied out of the employer's pocketbook. Accordingly if a employer funded health plan violated the HIPAA Privacy Rules by disclosing confidential information to the employer, liability for breach of confidentiality would nearly always pass through to the employer.

Employers as plan sponsors may access an employee's protected health information in order to make employment decisions only with the formal authorization of the concerned employee. [FN256] However, the Rules do not appear to

allow employers to require as a condition of employment that their employees execute authorization forms for this purpose. The HIPAA Privacy Rules prohibit covered entities conditioning provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the execution of an authorization form. [FN257] Thus, if employers do not end the practice of using employee health information to make employment decisions, they are likely to become far more common than doctors, hospitals and insurance companies as defendants in breach of confidentiality actions.

***672** E. Downstream Liability for Business Associates

As we have seen, other than a possible breach of contract claim by the covered entity, the Rules do not make business associates of covered entities liable for misuse of protected health information. Since, as a practical matter, a tremendous amount of personal health information is handled and processed by business associates, the lack of express administrative or criminal sanctions for misuse of personal health information represents a gaping hole in the regulatory framework established by Congress. The Rules as they were originally proposed attempted to this regulatory gap by requiring that all contracts between covered entities and what the proposed rules called "business partners" of covered entities designate patients as the "third (-)party beneficiaries" of the contracts, with potential civil claims for breach of contract against business partners who violated the contracts. [FN258] After considerable controversy, this provision was withdrawn in the final rules and replaced with the concept of a "business associate" without such third party beneficiary liability. [FN259]

The problem of regulating the use of electronic personal health information-- whether by business associates or by covered entities--is, quite simply, the single most critical question presented today with respect to the law of health information. As we have seen, virtually all medical information used today exists widespread computer networks. Anyone the system can simply call an electronic medical record up on a screen. Professor Gostin argues that the rule of confidentiality worked well in the past when most of the intimate information was generated within the physician-patient relationship, but he asserts that the rule of confidentiality does not work nearly as well in a modern information society. [FN260] Instead, Gostin argues that the rule of confidentiality, which places the duty of care on the health care provider generating the record, must be replaced with a system of privacy in which legal protection is attached to the health record itself, not simply to the provider that generates it. [FN261] Since the HIPAA Privacy Rules are largely modeled on a rule of confidentiality, Gostin's argument appears particularly compelling when addressing the failure of the Rules to hold business associates accountable for misuse of personal health information.

***673** This Article represents a defense of the rule of confidentiality in the field of health information law. The defense is partly based on a belief that the doctrinal system of breach of confidentiality theory is capable of controlling the misuse of health information in cyberspace, a belief that trying to regulate entities and individuals is more practical than trying to regulate information, itself, and finally by a concern that the attempt to regulate information outside of the context of a relational system of duties may well be unconstitutional.

Breach of confidentiality can remain a viable legal means to protect electronic health care information. Even in cyberspace, that most downstream users of medical information access electronic health information from upstream health care providers that are under a traditional duty of confidentiality. In the context of the HIPAA Privacy Rules, no business associate can obtain any personal health information from a health care provider or payer without executing a "business associate contract." [FN262] Even before the HIPAA Rules, downstream users were on notice that they also were expected to abide under the same rule of confidentiality owed patients by a doctor or a hospital. The common law "inducement" to breach of confidentiality tort placed a duty on a third party who had notice that health information was obtained through a confidential relationship. The fairness of applying such duties to third parties did not come from the sensitive nature of the information itself, but was derivative of the duty of confidentiality of the health care provider. In effect, the common law cases imply that the "downstream" party assumed a duty of confidentiality when they acquired

this information from the provider. [FN263]

Under the Rules, with the requirement of a written contract, it is much easier to prove that the party acquiring information downstream--the business associate--assumed the duty of confidentiality from the provider or payer, for the agreement is no longer implied but express. Thus, under the Rules, all downstream users of medical information under contracts with the covered entities expressly have agreed to a duty to maintain the confidentiality of any personal health information they obtain from covered entities. As such, it appears likely under the developing case law, that business associates assume potentially liability if they breach that duty. The Rules may not create a private cause of action to patients for misuse of their personal health information, but a private cause of action already exists in ***674** the common law. Under the common law, making downstream entities liable was perceived to be unfair without proof that the downstream entity had assumed a duty of confidentiality. If all business associates must agree to rules of confidentiality before they can obtain personal health information from covered entities, the Rules greatly simplify this proof.

Thus the Rules promise to transform an action against a downstream entity for breach of confidentiality into a simple application of agency theory. If there is a confidentiality contract between covered entities and their business associates, business associates become agents of the covered entities with respect to their use and management of personal health information on behalf of the covered entity. General agency law makes the agent liable to a third party for the violation of a duty owed the third party by the principal. [FN264] The covered entity, as the principal, may well have a defense of the exercise of reasonable care that can be shown by a contract requiring the business associate to protect personal health information according to the standards of the HIPAA Privacy Rules. However, the failure by the business associate to conform to the standards set forth in the Rules, after the agent's execution of a business associate contract, may allow a plaintiff injured by misconduct by a business associate to establish tort liability under the common law tort breach of confidentiality.

F. Confidentiality and the First Amendment

In recent years, attempts by lawmakers to protect personal information with rules which create a "right of privacy" have often receive withering constitutional scrutiny by the Supreme Court. [FN265] In a thought-provoking article in the Stanford Law Review, Professor Eugene Volokh explores the negative implications of making downstream users of personal information liable for the disclosure of that information under the rubric of protection of an individual right to privacy. [FN266] It would appear that any attempt to attach a ***675** right of privacy to the medical record itself would receive similar unfriendly constitutional scrutiny.

In this context, the application of breach of confidentiality theories to protect personal health information "downstream" raises the question whether such tort theories may also be in tension with the First Amendment. At least two other articles have concluded that the breach of confidentiality tort would be subject to a strong, if not fatal, challenge under the First Amendment. [FN267]

One of the clearest expressions of the constitutional infirmity of attempts to regulate information under the rationale of protecting privacy is found in Justice Stevens' recent plurality opinion of Bartnicki v. Vopper. [FN268] Bartnicki involved a suit against a radio station for its broadcast of an illegally intercepted telephone call under the provisions of the Electronic Communications Privacy Act, [FN269] which created a civil cause of action against any person who, knowing or having reason to know that a communication was obtained through an illegal interception, willfully disclosed its contents. [FN270] The Court held that to the extent that the statute purported to create liability for publishing lawfully obtained information from a source who obtained it unlawfully, the statute violated the First Amendment's protection of freedom of speech. [FN271] In his plurality opinion striking down the statute, Justice Stevens noted "the naked prohibition against disclosures is fairly characterized as a regulation of pure speech." [FN272] Stevens further noted that

"(a)s a general matter, 'state action to punish the publication of truthful information seldom can satisfy constitutional standards."' [FN273] Stevens continued by saying, "This Court has repeatedly held that 'if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order."' [FN274] ***676** The opinion in Bartnicki can be considered limited to matters of public concern and not to prohibit laws protecting speech that involve matters merely of private concern, given the separate concurrence by Justices Breyer and O'Connor who attempt to leave room for other legal attempts to protect personal privacy by regulating disclosures of information. [FN275] However, Bartnicki still appears to raise a significant obstacle to any attempt to create a general "right of privacy" in personal information under the First Amendment.

It is the thesis of this Article that to the extent that the HIPAA Privacy Rules attempt, in the words of Professor Gostin, "to attach protection to the health record itself, rather than to the institution that generates it," [FN276] the protections created by the Rules would appear to be subject to constitutional attack under the First Amendment. [FN277] However, if the HIPAA Rules are understood as implementing a regime in which personal health information is protected in the context of professional and contractual relationships of trust, the constitutional concerns diminish under legal theory and Supreme Court case law.

It should be noted again that confidentiality and privacy are different legal concepts. Rules fashioned to protect the confidentiality of health information are based on different jurisprudential assumptions from rules protecting privacy. Confidentiality of health information is based on a relationship of trust between the doctor and the patient. Privacy of health information is not dependent on the existence of a relationship of trust, but derives from the intimate and personal nature of the information itself. The right of privacy in health information is analogous to a property right in information--where it exits, it gives individuals control, to a greater or lesser degree, over the use, access and disclosure of their individually identifiable health information, independent of their relationship with a healthcare provider. Bartnicki can be read as indicating that a general right of privacy in information is inherently problematic under the First Amendment. However, the Rules should be understood not as creating a "right of privacy" in information but implementing well-known and ***677** established duties of confidentiality on the part of covered entities and business associates who have expressed agreed to assume such a duty. The Rules do not regulate personal health information based on the private nature of that information, but only regulate the relationships in which such information is exchanged.

In the decisions of the Supreme Court, the clash between the protection of information and the First Amendment interest in free expression appears to be sharpest when there is no pre-existing relationship between the subject of the information and the person disclosing the information that could give rise to an explicit or implicit expectation of confidentiality. There appears to be a presumption that laws which place duties of non-disclosure when there exists an independent duty or relationship of trust are constitutional, but that laws placing duties of non-disclosure on individuals and entities when no such relationship of trust exists appear to be presumptively unconstitutional. This distinction was first implied in a footnote in Landmark Communications, Inc. v. Virginia. [FN278] The distinction was made express in Cohen v. Cowles Media, [FN279] when the Supreme Court held that the First Amendment did not prohibit a news source from recovering damages from a newspaper publisher under a theory of promissory estoppel for publishers' breach of promise of confidentiality given in exchange for the information. [FN280] In Cohen, the Court held that the First Amendment does not give the press the right to disregard promises which otherwise would be enforceable under state law. [FN281]

Although the Rules contain the word "privacy" in their title, properly understood, they do not create any true "right to privacy" in health information. The Rules adopt a traditional confidentiality model of regulation of personal health information. The Rules do not apply until there exists a previously existing professional or contractual relationship between patient and healthcare provider. The Rules do not create a general right to control the disclosure of personal

health information, they do not regulate information, they only regulate relationships.

***678** As we have seen, the HIPAA Privacy Rules generally codify at a federal level the same standards of confidentiality based on relationships of trust established by state common law. Both the common law tradition of confidentially and the HIPAA Privacy Rules begin with a general presumption that information generated in the context of a relationship with a healthcare provider is entitled to a strong general rule of protection. Exceptions are then made permitting limited disclosures for specific purposes with the understanding that those to whom personal health information is disclosed stand in a "chain of trust" with respect to this information. In this respect, the Rules do not establish a new set of legal requirements, but merely serve as a federal codification of traditional state common law confidentiality doctrines. Even the most novel portion of the Rules--their implementation of fair information practices--uses relationship-based structures of confidentiality; they do not create rights to control information characteristic of a "right of privacy." The Rules articulate the scope of duties in the context of specific professional and contractual relationships of confidentiality--those between patient and physician--and secondary relationships of confidentiality between the physician and other healthcare providers, payers, and business associates. As the Supreme Court in Cohen v. Coles Media has made clear, regulation of the use and disclosure of personal health information within the context of a contractual or professional promises of confidentiality appears to present much less pressing constitutional concerns. The primary relationships governed by the Rules are those professional and contractual relationships between patients and healthcare providers, healthcare providers and plans, and patients and clearinghouses. The secondary relationships governed by the Rules are those between covered entities such as healthcare providers, plans, and clearinghouses; and business associates. None should be considered constitutionally problematic.

In the context of a such a system of relationships between a patient and a healthcare provider, and between a patient and a health insurer, the First Amendment does not appear to prohibit the government from setting a default rule of non-disclosure in the absence of express written consent to the contrary. If the healthcare provider or insurer then contracts with a third party to process such restricted personal health information, the First Amendment also should not prohibit the government from deeming the third party to be an agent of the first business, bound by the same rules of confidentiality as its principal as to the treatment of the personal information. Thus, as to personal information for which there is no express written consent from the patient, if a third party obtains personal health ***679** information in the context of an explicit or implicit obligation of confidentiality, and breaches this duty of confidentiality by further disclosing the information for its own purposes, the First Amendment does not prevent the law of agency from making the third party potentially liable to the harmed consumer. While the First Amendment does appear to limit the government's ability to establish liability in the absence of a contractual or professional duty, the Supreme Court has shown itself to be extremely deferential in the constitutional review of legal enforcement of non-disclosure agreements when such agreements are in the context of an independent and legitimately established relationship of confidentiality. [FN282] In general, within the culture of the healthcare industry, it is well understood that business associates that misuse personal health information do so in violation of their contractual duties to covered entities as well as to the patients. As such, the application of breach of confidentiality theories to such entities does not raise the same constitutional concerns as many other attempts to protect information under the rationale of a "right to privacy."

G. Costs and Benefits

It is the thesis of this Article that the Rules do not represent a dramatic alteration in the rules governing healthcare providers. The extremely high cost estimates associated with their implementation are a matter of considerable interest. [FN283] While the application of fair information practices in the context of personal health information may be responsible for some of the increase in costs, prior to the enactment of the Rules at least twenty-eight states already provided a right for patients to review their medical records and to recommend changes or amendments if necessary. [FN284] Various federal health benefit programs such as the Medicare program also imposed similar requirements.

[FN285] If the duties placed on health care providers were not substantially altered by the implementation of HIPAA Privacy Rules, then HIPAA may not be responsible for the high estimated costs of compliance. The most likely explanation of the increase in costs associated with the ***680** implementation of the HIPAA Privacy Rules appears to be the fact that, in recent years, many healthcare providers have invested significant resources in increasingly accessible computerized health information networks without maintaining appropriate safeguards to protect medical information as the accessibility of health information increased. As we have seen, traditional standards for confidentiality that involved only modest costs when information was stored in locked file cabinets, or in main frame computers, now present much more difficult and expensive information management problems in the context of vast national electronic health networks. Thus, the high cost estimates associated with the HIPAA Privacy Rules appear to be due simply to the exponential growth in the use of electronic health information by the health care industry without a concomitant investment in compliance with previously existing duties of confidentiality. If this is the reason for the large cost estimates, the Rules have had the salutary impact of causing an extremely large sector of the American economy to wake up to the fact that the benefits that are obtained from the growth in the use of electronic health information also bring with them potential dangers.

The task of balancing the benefits of electronic health information against the risks of disclosure will be handled in large part not by administrative agencies and federal prosecutors, but in the same manner as the risks of disclosure in a simpler age were handled--by common law courts in fact-specific cases. The fact that the high cost-estimates of compliance with HIPAA appear to be self-inflicted does not resolve the question whether a possible cost of expanding private causes of action under breach of confidentiality theories would be outweighed by the potential benefits. In other words, does expansion of liability for breach of confidentiality make economic sense?

In this context, it is important also to note that the greatest dangers associated with the disclosure of health information occur not when the information is disclosed to strangers, but when it is disclosed within a community. Disclosure of adverse health information to an employer is far more likely to involve dangers to the patient than disclosure of the same information in the context of treatment and payment decisions, research, public health reviews, and licensing oversight of healthcare providers, all of which disclosures usually take place to public officials who usually are strangers within the individual's community. An anonymous stranger who processes health claims or who conducts statistical medical research is in a less dangerous position to the patient than someone who knows the patient personally and is in a position to use it in a way that affects the patient's life. Even if the person close to the patient operates with the best of intentions, ***681** his acquisition of sensitive medical information may be more threatening than unauthorized access to medical records by a stranger. The disclosure to a stranger who does not know or care about the patient simply does not involve the same risks as the disclosure of health information within or among a community, family, friends, neighbors, customers, and clients.

There is clearly a sense in which inadvertent disclosure of personal health information to a janitor at a physician's office can be said to constitute a "breach of confidentiality." However, if the stranger to whom personal health information is disclosed in turn keeps the information "confidential" in a chain of trust, or fails to disclose it further because of a lack of interest, there is little harm done by such breaches of confidentiality. On the other hand, if the personal health information makes its way back to the patient's community, the risk of damage to the patient from the disclosure increases significantly and there is a sense that the chain of trust has been broken.

A system of legal rules ideally should encourage the holder of information to weigh the risk of harmful disclosure against the resources that must be invested in information management to protect against such possible disclosure. Fundamentally, the result should be a pragmatic balancing of risks and benefits. The ultimate goal is to protect the patient's trust in the integrity of his or her medical information consistent with the needs for disclosure of that information for purposes of treatment, payment, oversight, and other socially important uses. The common law doctrine of breach

of confidentiality seems to be an appropriate vehicle to establish an appropriate allocation of social resources for this purpose. In general, liability should be limited in the absence of damages. The common law operates under a "no harm, no foul" approach. Unauthorized access, even by strangers, that does not result in any misuse of information, and which does not result in embarrassing disclosures within a community, may not be actionable, or if actionable, should result in an award of nominal damages.

The review of individually-identifiable medical information by a stranger with no ulterior purpose other than processing a claim, review of drug interactions, the identification of lower-cost alternatives, or education of the provider or patient do not present any serious likelihood of damage to the subject of that information. The possibility that cleaning staff may access confidential patient health information should not necessarily cause the expenditure of massive social resources if there is little likelihood that the information will be misused. The common law standard of care permits the health information manager to exercise some discretion in determining who ***682** is given access to health information in the course of treatment. The common law's requirement that there be a showing of actual harm from the disclosure of individual health information places an appropriate degree of responsibility on the health information manager to appropriately balance the cost of additional protections of information against the potential dangers of harmful disclosure.

VI. Conclusion

In summary, both the common law rule of confidentiality and the HIPAA Privacy Rules adopt a model based on the tort law concept of the balancing of costs and benefits. The common law tort of breach of confidentiality is likely to have more, rather than less, relevance in an age when the risks of disclosure of electronic medical information have increased. Furthermore, the close relationship between the HIPAA Privacy Rules and the common law indicates that there will be significant interaction between the two bodies of law as breach of confidentiality cases are litigated in the future.

[FNa1]. Adjunct Instructor, Dedman Law School, Southern Methodist University; Assistant U.S. Attorney, U.S. Department of Justice; J.D., Harvard Law School; M. Phil. Philosophy, University College, London; B.A., Williams College. The views expressed in this article are the personal views of the author alone and should not be considered in any way to represent the views of the United States Department of Justice. In preparing this Article, I received suggestions, comments and support from Richard Turkington, Alan Westin, John B. Attanasio, Michael Froomkin, Jonathan Simon, Eugene Volokh, Dan Solove, Marc Rotenberg, Peter Swire, Mark Rothstein, Tim Webster and Jane Winn.

[FN1]. 45 C.F.R. § 164.500--164.534 (2001).

[FN2]. 42 U.S.C. § 1320d to 1320d-8 (2002).

[FN3]. See Dept. of Health and Human Servs., Final Privacy Rule Preamble-- Background and Purpose, at http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm (last visited Apr. 19, 2002); see also Secretary of Health and Human Services; Recommendations, Confidentiality of Individually-identifiable Health Information, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996 (Sept. 11, 1997) (hereafter the "Secretary's Recommendations").

[FN4]. 42 U.S.C. § 1320d-2(d)(2). The Rules were issued in the context of two other closely related federal regulations, one establishing nationwide standardized data sets and the other establishing national security standards for electronic health information. See 65 Fed. Reg. 82462 (Dec. 28, 2000) and 65 Fed. Reg. 50312 (Aug. 17, 2000).

[FN5]. 45 C.F.R. § 160.103.

[FN6]. 45 C.F.R. § 164.502(e).

[FN7]. See Comm. on Maintaining Privacy and Sec. in Healthcare Applications of the Nat'l Info. Infrastructure & Computer Sci. and Telecom. Bd., Nat'l Research Council, For the Record: Protecting Electronic Health Information (1997), available at http://books.nap.edu/books/0309056977/html/index.html (last visited Apr. 4, 2002) ("Protecting Electronic Health Information"); Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of United States Data Protection § 7-3 (1996); Robert M. Gellman, Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy, 62 N.C. L. Rev. 255 (1984); Lawrence O. Gostin, Health Information Privacy, 80 Cornell L. Rev. 451 (1995). But see G. Michael Harvery, Comment, Confidentiality: A Measured Response to the Failure of Privacy, 140 U. Pa. L. Rev. 2385 (1992).

[FN8]. This criticism of the breach of confidentiality tort was first made in the seminal 1890 law review article by Louis D. Brandeis and Samuel D. Warren, entitled The Right to Privacy, 4 Harv. L. Rev. 193 (1890):
So long as these circumstances happen to present a contract upon which such a term can be engrafted by the judicial mind, or to supply relations upon which a trust or confidence can be erected, there may be no objection to working out the desired protection through the doctrines of contract or of trust. But the court can hardly stop there. The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.
Id.

[FN9]. 501 U.S. 663 (1991)

[FN10]. The Hippocratic Oath reads in part, "And whatsoever I shall see or hear in the course of my profession, as well as outside of 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." Vol. 1 Hippocrates 301 (W.H.S. Jones ed., 1995).

[FN11]. The American Medical Association's Code of Medical Ethics provides that "the physician should not reveal confidential communications or information without the express consent of the patients." AMA Code of Medical Ethics § 5.05 (1996-1997).

[FN12]. For an excellent discussion of the various forms of disclosure of medical records within the healthcare industry see Alan Westin, U.S. Dep't of Commerce, Nat'l Bureau of Standards, A Policy Analysis of Citizen Rights Issues in Health Data Systems: Issues in Health Data Systems 1-13 (Florence Isbell ed., 1977). This work also contains one of the earliest analyses of the threat to medical confidentiality created by the computerization of medical records.

[FN13]. The writings of Hippocrates are themselves a testament to how experienced physicians trained and consulted with less experienced medical students through observation of individual patients. See generally, Vol. 1 Hippocrates, 313-33 (W.H.S. Jones trans., 1995).

[FN14]. Robert Ellis Smith, War Stories 54-59 (1997).

[FN15]. Arthur Allen, Exposed, Washington Post Magazine (Sunday, Feb. 3, 1998).

[FN16]. Originally designed for use by physicians to bill Medicare and Medicaid programs, the Form CMS-1500 (formerly HCFA-1500)--issued by the Centers for Medicare and Medicaid Services (formerly the Health Care Financing

Administration) is universally used as the standard health insurance claim form throughout the health care industry. See http://www.hhs.gov. The Form CMS-1500 requires the physician to identify a specific diagnosis code (International Classification of Diseases or ICD-9 Code) and a specific treatment code (Current Procedural Terminology Code or CPT-Code) in order to secure payment for the medical service. See, American Medical Association, Physician ICD-9-CM (2002); and American Medical Association CPT Professional Edition (2002).

[FN17]. See, e.g., Texas Occupations Code, Chapter 159.003(a)(5) (2002) (providing for disclosure of records subject to physician-patient confidentiality in context of physician disciplinary investigations).

[FN18]. See, e.g., http://cms.hhs.gov/glossary (Description of Peer Review Organizations that provide oversight functions for the Medicare program); Texas Occupation Code, Chapter 160, §§ 160.001-160.010 (2002) (Requirements Relating to Medical Peer Review).

[FN19]. For the Record, Protecting Electronic Health Information 66 (1997).

[FN20]. In a March 1996 consent degree filed in Minnesota and joined by 17 other states, one PBM agreed to stop interfering in the prescription of medications from other manufacturers when it assessed patients' eligibility for coverage. PRNewswire. 1996. "Minnesota Takes the Lead on Agreement to Protect 41 Million Americans." October 25. www.epic.org/privacy/medical/merck.txt.

[FN21]. Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse. GAO-HRD-92-69 (1992). See also, Malcolm K. Sparrow, License to Steal: Why Fraud Plagues America's Health Care System (1996).

[FN22]. National Health Care Expenditures Projections: 2000-2010, Report of the Office of the Actuary, Health Care Financing Administration (2001).

[FN23]. See, e.g., Fed. R. Crim. P. 6(e) (Grand Jury Secrecy Rules); 18 U.S.C. § 3486(e) (2002) (administrative subpoena confidentiality provisions).

[FN24]. See generally Lawrence O. Gostin, Public Health Law: Power, Duty, Restraint 117 (2000).

[FN25]. Id. at 117-18.

[FN26]. See, e.g., Whalen v. Roe, 429 U.S. 589 (1977).

[FN27]. See, e.g., N.Y. Pub. Health § 2130. For an excellent general discussion of public health surveillance, reporting requirements and partner notification, see, Gostin, supra note 24, at 116-23.

[FN28]. Anthony G. Macintyre et al., Weapons of Mass Destruction: Events with Contaminated Casualties, 238 JMAM 242 (2000); Centers for Disease Control & Prevention, Bioterrorism Alleging Use of Anthrax and Interim Guidelines for Management, 281 JAMA 787 (1999).

[FN29]. See, e.g., McCormick v. England, 328 S.C. 627, 642-643 494 S.E.2d 431, 439 (1998)(Listing South Carolina disclosure requirements). See also, Texas Occupation Code § 159.003(2) (permitting disclosure when physician determines there is a probability of imminent physical injury to a third person).

[FN30]. See, e.g., Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334 (Cal. 1976).

[FN31]. 551 P.2d 334 (Cal. 1976).

[FN32]. Id. at 343, 351.

[FN33]. See, McCormick v. England, 328 S.C. 627, 641-43, 494 S.E.2d 431, 438-39 (1998) (discussion of state reporting requirements).

[FN34]. See id. See also Gostin, supra note 24, at 137-38.

[FN35]. See id. at 121-25.

[FN36]. For an excellent discussion of the controversy concerning partner notification and reporting, see id.

[FN37]. See e.g., Whalen v. Roe, 429 U.S. 589 (1977); U.S. v. Westinghouse, 638 F.2d 570 (3d Cir. 1980).

[FN38]. Gostin, supra note 24, at 139-42.

[FN39]. Protection of Human Subjects, 45 C.F.R. § 46.101 to 404 (1993) (Also known as the "Common Rule").

[FN40]. See, e.g., Ralph L. Rosnow et al., The Institutional Review Board as a Mirror of Scientific and Ethical Standards, 48 Am. Psychologist 821, 821- 26 (1993).

[FN41]. Id.

[FN42]. See, Department of Heath & Hum. Servs. Office of Inspector Gen., Institutional Review Boards: A Time for Reform (1998); Gostin, supra note 24, at 125-26.

[FN43]. Richard C. Turkington, Medical Records Confidentiality Law, Scientific Research, and Data Collection in the Information Age, 24 J.L. Med. & Ethics 113, 115 (1997); see also Simson Garfinkel, Nobody Knows the MIB, in Database Nation: The Death of Privacy in the 21st Century 136-39 (2000).

[FN44]. National Research Council, For the Record: Protecting Health Information 32-33 (1997).

[FN45]. Id.

[FN46]. Simson Garfinkel, Nobody Knows the MIB, in Database Nation: The Death of Privacy in the 21st Century 137.

[FN47]. See Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. Ct. 1990) (holding a disclosure by an employer to other employees of an employee's mastectomy did state a cause of action under public disclosure tort); Young v. Jackson, 572 So. 2d 378, 385 (Miss. 1990) (holding a disclosure by employer to other employees of an employee's partial hysterectomy operation for a legitimate purpose and privilege).

[FN48]. 29 U.S.C. § 1144.

[FN49]. See generally, Wm. Sage, "Health Law 2000": The Legal System and the Changing Health Care Market, 15 Health Aff., No. 3, at 9 (Fall 1996).

[FN50]. Id.

[FN51]. See, e.g., David F. Linowes & Ray C. Spencer, Privacy: The Workplace Issue of the '90s, 23 J. Marshall L. Rev. 591, 593-94 (1990) (citing a survey of Fortune 500 companies).

[FN52]. 29 U.S.C. § 1132 (2002). See Mary Anne Bobinski, Unhealthy Federalism, 24 U.C. Davis L. Rev. 255 (1990); see also Mark A. Rothstein, Genetic Discrimination in Employment and the Americans with Disabilities Act, 29 Hous. L. Rev. 23 (1992).

[FN53]. In the context of conducting genetic research on medical databases it is not always possible for researchers to obtain the consent of all the individuals whose medical records are studied. For a discussion of the ethical issues surrounding such studies, see generally, Ellen Wright Clayton, Informed Consent and Genetic Research, in Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era 126-36 (Mark A. Rothstein, ed. 1997).

[FN54]. National Research Council, Trust in Cyberspace, 14 (1999).

[FN55]. Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles For Providing and Using Personal Information, (June 6, 1995), available at http://www.iitf.nist.gov/documents/committee/infopol/niiprivprin_final.html (last visited Apr. 1, 2002).

[FN56]. See supra Part II. C. (discussion of "slack" in hospital confidentiality).

[FN57]. Alan F. Westin Et. Al., Health Care Information Privacy: A Survey of the Public and Leaders 18-19 (1993) (survey conducted for Equifax, Inc.). The study finds that medical privacy receives the highest level of concern (48%) followed by consumer privacy (46%) and general privacy (25%).

[FN58]. In Weston's Health Information Privacy Survey, supra note 57, at 66- 67, 29% of the respondents stated that the fact that their health care providers use computers concerns them; strong majorities felt that computer use causes billing mistakes (75%), leads to inaccurate recordings of medical conditions (60%), and facilitates unauthorized disclosure of sensitive information (63%).

[FN59]. See e.g., Robert Ellis Smith, War Stories, 54-59 (1997).

[FN60]. 45 C.F.R. § 164.500-164.534 (2001).

[FN61]. See Gramm-Leach-Bliley Act (also known as Financial Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338, 15 U.S.C.A. § 6801 et seq. (2002); Children's Online Privacy Protection Act of 1998, 15 U.S.C. 501 (1999); Telecommunications Act of 1996, Pub. L. No. 104-104 § 502, 110 Stat. 56; Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994).

[FN62]. 42 U.S.C. § 1320d-2 and 1320-d-4 (2002).

[FN63]. Section 264 of HIPAA is found as a note to 42 U.S.C. § 1320d-2. The statute provides:
(a) In general.--Not later than (Aug. 21, 1996), the Secretary of Health and Human Services shall submit to the (Congress) detailed recommendations on standards with respect to the privacy of individually-identifiable health information.
(b) Subjects for recommendations.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually-identifiable health information should have.
(2) The procedures that should be established for the exercise of such rights.
(3) The uses and disclosures of such information that should be authorized or required.
(c) Regulations.--
(1) In general.--If legislation governing standards with respect to the privacy of individually-identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) (subsec.(a) of this section) is not enacted (by Aug. 21,1996), the Secretary of Health and Human Services shall promulgate final regulations containing such standards (by February, 2000). Such regulations shall address at least the subjects described in subsection (b)
Id. (citation omitted) (third alteration in original).

[FN64]. See Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (Nov. 3, 1999) (to be codified at 45 C.F.R. Parts 160 and 164).

[FN65]. See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,566 (Dec. 28, 2000).

[FN66]. One private study placed a price tag of $43 billion on the Rules. Robert E. Nolan Company, Inc., Cost and Impact Analysis: Common Components of Confidentiality Legislation 2 (Fall 1999), (accessible at http:// ww.renolan.com/healthcare/privacy.htm) ("The Nolan Study").

[FN67]. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82461-82829 (December 28, 2000) (to be codified at 45 C.F.R. Parts 160 and 164).

[FN68]. Request for Comments, 66 Fed. Reg. 12,738 (February 28, 2001).

[FN69]. Statement by HHS Secretary Tommy G. Thompson Regarding the Patient Privacy Rule, HHS News, U.S. Department of Health and Human Services (April 12, 2001), available at http://www.hhs.gov/news/press/2001pres/20010412.html (last accessed June 30, 2002).

[FN70]. 67 Fed. Reg. 14776-14815 (March 27, 2002) (to be codified at 45 C.F.R. Parts 160 and 164).

[FN71]. In Association of American Physicians and Surgeons, Inc. et al. v. United States Department of Health and Human Services, et al., No. H-01- 2963 (Jun. 17, 2002), the District Court upheld the Rules. See also S.C. Med. Ass'n v. U.S. Dep't of Health & Human Servs., No. 3:01-2965-19 (D. S.C. filed July 31, 2001) (pending request for declaratory relief).

[FN72]. See The Nolan Study, supra note 66.

[FN73]. 45 C.F.R. § 164.534(a).

[FN74]. 45 C.F.R. § 164.534(b)(2).

[FN75]. 67 Fed. Reg. 14815 (to be codified at 45 C.F.R. § 164.534).

[FN76]. Subtitle F of Title II of HIPAA consists of sections 261 through 264. Those sections are codified at 42 U.S.C. § 1320d to 1320d-8 (2002). The regulations are codified at 45 C.F.R. Parts 160, 162 and 164.

[FN77]. Section 261 is found as a note to 42 U.S.C § 1320d ("It is the purpose of this subtitle...to improve...the efficiency and effectiveness of the health 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.").

[FN78]. 42 U.S.C. § 1320d-2 (2001); 45 C.F.R. § 501.

[FN79]. 42 U.S.C. § 1320d-7.

[FN80]. 42 U.S.C. § 1320d-1(a).

[FN81]. 42 U.S.C. § 1320d(3); 45 C.F.R. § 160.103.

[FN82]. Id.

[FN83]. Id.

[FN84]. 42 U.S.C. § 1320d(5); 45 C.F.R. § 160.103.

[FN85]. Id.

[FN86]. Id.

[FN87]. 42 U.S.C. § 1320d(2); 45 C.F.R. § 160.103.

[FN88]. 42 U.S.C. § 1320d(6); 45 C.F.R. § 164.530.

[FN89]. Id.

[FN90]. Id.

[FN91]. 45 C.F.R. § 164.501.

[FN92]. 42 U.S.C. § 1320d(6); 45 C.F.R. § 501.

[FN93]. Id. § 164.514(b)(2)(i).

[FN94]. 67 Fed. Reg. 14798 to 14800 (March 27, 2002) (to be codified at 45 C.R.R. 164.514).

[FN95]. 45 C.F.R. § 164.506 (2001).

[FN96]. 67 Fed. Reg. 14778 to 14781 (March 27, 2002) (to be codified at 45 C.F.R. § 154.506).

[FN97]. Id.

[FN98]. Id. As a practical matter, many health care providers will continue to use consent forms as a matter of tradition or because of state law requirements.

[FN99]. 45 C.F.R. § 164.512(a)-(k).

[FN100]. 45 C.F.R. § 164.512.

[FN101]. Supra Part II. E. 1.

[FN102]. 45 C.F.R. § 164.508.

[FN103]. 67 Fed. Reg. 14797-14798.

[FN104]. 45 C.F.R. § 164.508.

[FN105]. Id.

[FN106]. 45 C.F.R. § 164.508(a)(2).

[FN107]. Id. § 164.508(b)(4).

[FN108]. Id. § 164.508(b)(5).

[FN109]. See Turkington, supra note 43. at 119.

[FN110]. See id.

[FN111]. 67 Fed. Reg. 14789-14791 (to be codified at 45 C.F.R. § 164.501).

[FN112]. Id.

[FN113]. 45 C.F.R. 164.508(f).

[FN114]. 67 Fed. Reg. 14793 to 14796.

[FN115]. 45 C.F.R. 164.508(f).

[FN116]. 67 Fed. Reg. 14795 (to be codified at 45 C.F.R. § 164.508(f)).

[FN117]. Id.

[FN118]. 45 C.F.R. § 502(b); see also 45 C.F.R. § 164.502(b)(1).

[FN119]. Department of Health and Human Services, 65 Fed. Reg. 82,462, at 82,714 (Dec. 28, 2000) (noting that the final regulations do not require "all reasonable efforts" as required by the proposed regulations).

[FN120]. 67 Fed. Reg. 14784 to 14787 (to be codified at 45 C.F.R. § 502(b)(1)).

[FN121]. 67 Fed. Reg. 14786.

[FN122]. Id.

[FN123]. Id.

[FN124]. See generally Alan F. Westin, Privacy and Freedom 158-168 (1967); Alan F. Westin & Michael A. Baker, Databanks in a Free Society: Computers, Recordkeeping and Privacy 229 (1972); Arthur R. Miller, Computers, Data Banks and Individual Privacy: An Overview, 4 Colum. Hum. Rts. L. Rev. 1, 1-10 (1972).

[FN125]. U.S. Dep't of Health, Educ., and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems ("HEW Report") (1973).

[FN126]. The HEW Report reads as follows:
There must be no personal-data record-keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
Id. at xx-xxi.

[FN127]. Id.

[FN128]. 5 U.S.C. § 552a (1996).

[FN129]. 20 U.S.C. § 1232g (1988).

[FN130]. 18 U.S.C. § 2710 (1988).

[FN131]. See, generally, Convention For the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108; Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58 (1980).

[FN132]. 45 C.F.R. § 164.520 (2001).

[FN133]. Id. § 164.524.

[FN134]. Id. § 164.526(a).

[FN135]. Id. §§ 164.528(a)(1), (1)(i).

[FN136]. Id. § 164.530(d).

[FN137]. Id. § 164.530.

[FN138]. Id. § 160.103.

[FN139]. Id.

[FN140]. Id.

[FN141]. Id. § 164.504(e).

[FN142]. Id. § 164.504(e)(2).

[FN143]. 42 U.S.C. § 1320d-5(a).

[FN144]. Id.

[FN145]. 42 U.S.C. § 1320-6.

[FN146]. Id.

[FN147]. 45 C.F.R. § 164.504(e).

[FN148]. Purpose of the Administrative Simplification Provisions, 65 Fed. Reg. 82,472-82,473 (December 28, 2000).

[FN149]. Secretary's Recommendations 2, supra note 3.

[FN150]. The Restatement (Second) of Torts summarizes the types of situations in which a cause of action for invasion of privacy arises:
(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
(2) The right of privacy is invaded by
(a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
(b) appropriation of the other's name or likeness, as stated in § 652C; or
(c) unreasonable publicity given to the other's private life, as stated in § 652D; or
(d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.
Restatement (Second) of Torts § 652A (1976).

[FN151]. Porten v. Univ. of San Francisco, 64 Cal. App.3d 825, 828-829, 134 Cal. Rptr. 839, 841 (Cal.App. 1 Dist. 1976). For criticisms of the requirement of widespread publication, see Miller v. Motorola, Inc., 560 N.E.2d 900, 902 (Ill. App. Ct. 1990). See also William Prosser & Page Keeton, Prosser and Keeton on the Law of Torts § 117 (5th ed. 1984).

[FN152]. See, Restatement (Second) of Torts § 652D.
One who gives publicity to a matter concerning the private life of another is subject to liability for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

[FN153]. Id.; See also, Turkington and Allen, Privacy Law, Cases and Materials 416-22 (1999).

[FN154]. See, e.g., Simonsen v. Swenson, 177 N.W. 831 (Neb. 1920).

[FN155]. See, e.g., Hammonds v. Aetna Cas. & Sur. Co., 243 F.Supp. 793 (N.D. Ohio 1965); Horne v. Patton, 287 So. 2d 824 (Ala. 1973); Vassiliades v. Garfinckel's, 492 A.2d 580 (D.C. 1985); Leger v. Spurlock, 589 So. 2d 40 (La. Ct.

App. 1991); Alberts v. Devine, 479 N.E.2d 113 (Mass. 1985), Saur v. Probes, 476 N.W.2d 496 (Mich. Ct. App. 1991); Brandt v. Med. Def. Assocs., 856 S.W.2d 667 (Mo. 1993) (en banc); Simonsen v. Swenson, 177 N.W. 831 (Neb. 1920); Hague v. Williams, 37 N.J. 328, 181 A.2d 345 (1962); Estate of Behringer v. Med. Ctr. at Princeton, 249 N.J.Super. 597, 592 A.2d 1251 (Law Div. 1991); MacDonald v. Clinger, 446 N.Y.S.2d 801 (N.Y. App. Div. 1982); Humphers v. First Interstate Bank, 696 P.2d 527 (Or. 1985) (en banc); McCormick v. England, 494 S.E.2d 431 (S.C. 1998); Schaffer v. Spicer, 215 N.W.2d 134 (S.D. 1974); Berry v. Moench, 331 P.2d 814 (Utah 1958); Morris v. Consolidation Coal Co., 446 S.E.2d 648 (W. Va. 1994). Only Tennessee has not expressly permitted recovery for a physician's breach of the duty of confidentiality. See, e.g., Quarles v. Sutherland, 389 S.W.2d 249, 252 (Tenn. 1965). However, some cases acknowledge the existence of a physician's duty of confidentiality. See, e.g., Shadrick v. Coker, 963 S.W.2d 726, 735 (Tenn. 1998); Roberts v. Chase, 166 S.W.2d 641, 650 (Tenn. Ct. App. 1942). See generally Alan B. Vickery, Note, Breach of Confidence: An Emerging Tort, 82 Colum. L. Rev. 1426 (1982).

[FN156]. See McCormick v. England, 328 S.C. 627, 636, 494 S.E.2d 431, 435-436; Alberts v. Devine, 395 Mass. 59, 479 N.E.2d 113, 119 (1985); Vassiliades v. Garfinckel's, 492 A.2d 580, 590 (D.C. 1985).

[FN157]. See McCormick v. England 328 S.C. 636, 494 S.E.2d 435-436 for discussion of case law in other jurisdictions.

[FN158]. 177 N.W. 831 (Neb. 1920).

[FN159]. Id. at 831.

[FN160]. Id.

[FN161]. Id. at 832.

[FN162]. Id. at 833.

[FN163]. 287 So. 2d 824 (Ala. 1973).

[FN164]. Id. at 825.

[FN165]. Id.

[FN166]. Id. at 829-30.

[FN167]. Id.

[FN168]. Id. at 829.

[FN169]. 181 A.2d 345 (1962).

[FN170]. Id. at 348.

[FN171]. Id.

[FN172]. Id.

[FN173]. 696 P.2d 527 (Or. 1985) (en banc).

[FN174]. Id. at 535.

[FN175]. Id.

[FN176]. Id.

[FN177]. Vickery, supra note 155, at 1451.

[FN178]. See, e.g. Horne v. Patton, 287 So. 2d 824 (Ala. 1973).

[FN179]. See, e.g., McCormick v. England, 328 S.C. 641-642, 494 S.E.2d 438-439 (citing case law in other jurisdictions).

[FN180]. Id.

[FN181]. Id. at 438 ("where the information disclosed is received in confidence, 'one can imagine many cases where the greatest injury results from disclosure to a single person, such as a spouse, or to a small group, such as an insurance company resisting a claim.'") (quoting Vickery, supra note 155, at 1442).

[FN182]. See Restatement (Second) of Torts § 652D.

[FN183]. See, e.g., McCormick v. England, 494 S.E.2d 431, 437-38 (S.C. 1997).

[FN184]. See id.

[FN185]. See id.

[FN186]. See id.

[FN187]. See id.

[FN188]. See Vickery, supra note 155, at 1441.

[FN189]. See Restatement (Second) of Torts § 652D and discussion of constitutional case law, infra, Part V. F.

[FN190]. McCormick, 494 S.E.2d at 438 (discussing Vickery, supra note 155, at 1440).

[FN191]. 177 N.W. 831 (Neb. 1920).

[FN192]. Id. at 833.

[FN193]. See McCormick v. England, 494 S.E.2d at 438-39; S.C. Code Ann. §§ 20-7-510,-540,-550 (Law Co-op. 1985 & Supp. 2001).

[FN194]. The Utah Supreme Court explained, "Where life, safety, well-being or other important interest is in jeopardy,

one having information which could protect against the hazard, may have a conditional privilege to reveal information for such purpose. . . ." Berry v. Moench, 331 P.2d 814, 817-18 (Utah 1958); see also Mull v. String, 448 So. 2d 952, 954 (Ala. 1984) (allowing disclosure of patient information when patient's health is at issue in litigation); Simonsen, 177 N.W. at 833 (holding the disclosure of information about a highly contagious disease is privileged and not a breach of the duty of confidentiality). In Saur v. Probes, the Michigan Court of Appeals found "(t)he issue whether the disclosures were reasonably necessary to protect the interests of (the) plaintiff or others is one for the jury (where) the facts are such that reasonable minds could differ." 476 N.W.2d 496, 499- 500 (Mich. Ct. App. 1991). In Estate of Behringer v. Med. Ctr. at Princeton, the New Jersey court discussed a variety of exceptions to the duty of confidentiality. 592 A.2d 1251, 1268-69 (N.J. Super. Ct. Law Div. 1991).

[FN195]. See, e.g., Whalen v. Roe, 429 U.S. 589, 601-602 (1977).

[FN196]. See supra Part II. E. 1.

[FN197]. See supra Part V. A.

[FN198]. 592 A.2d 1251 (N.J. Super. Ct. Law Div. 1991).

[FN199]. Id. at 1255-57.

[FN200]. Id. at 1271-74.

[FN201]. See id.1271-73.

[FN202]. Id. at 1271-73.

[FN203]. Id. at 1272-73.

[FN204]. Brandeis & Warren, supra note 3.

[FN205]. Gostin, supra note 7, at 508-13.

[FN206]. Id. at 512-13.

[FN207]. See, e.g., Humphers v. First Interstate Bank, 696 P.2d 527, 530 (Or. 1985) ("(O)nly one who holds the information in confidence can be charged with a breach of confidence.").

[FN208]. 243 F. Supp. 793 (N.D. Ohio 1965).

[FN209]. Id. at 795, 797-98.

[FN210]. Id. at 795.

[FN211]. Id.

[FN212]. Id. at 802.

[FN213]. Id.

[FN214]. Id. at 803.

[FN215]. See Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 528 (Ohio 1999).

[FN216]. 479 N.E.2d 113 (Mass. 1985).

[FN217]. Id. at 116.

[FN218]. Id. at 121 (citations omitted).

[FN219]. 446 S.E.2d 648 (W. Va. 1994).

[FN220]. Id. at 657-58.

[FN221]. Id. at 650.

[FN222]. Id. at 657.

[FN223]. 715 N.E.2d 518, 528 (Ohio 1999).

[FN224]. Id.

[FN225]. Id. at 520.

[FN226]. Id.

[FN227]. Id.

[FN228]. Id. at 528.

[FN229]. Id. at 524-25.

[FN230]. Secretary's Recommendations, supra note 3, p. 2. ("Any individual whose rights under the law have been violated, whether negligently or knowingly, should be permitted to bring an action for actual damages and equitable relief. For knowing violation attorney's fees and punitive damages should be available.").

[FN231]. 422 U.S. 66, later proceeding at 512 F.2d 909 (3d Cir. 1975), and questioned by Thompson v. Thompson, 484 U.S. 174, 188-92 (1988) (Scalia, J., concurring).

[FN232]. Id. at 78 (citations omitted) (emphasis in original).

[FN233]. See Transamerica Mortgage Advisors, Inc. v. Lewis, 444 U.S. 11 (1979); Touche Ross & Co. v. Redington, 442 U.S. 560 (1979).

[FN234]. See Middlesex County Sewerage Auth. v. Nat'l Sea Clammers Ass'n, 453 U.S. 1 (1981); Tex. Indus., Inc. v.

Radcliff Materials, Inc., 451 U.S. 630 (1981); California v. Sierra Club, 451 U.S. 287 (1981); Northwest Airlines, Inc. v. Transp. Workers Union, 451 U.S. 77 (1981).

[FN235]. ___ U.S. , 122 S.Ct. 2268 (2002).

[FN236]. 20 U.S.C. § 1232g (2002).

[FN237]. Id.

[FN238]. Gonzaga, 122 S.Ct. at 2279.

[FN239]. Id.

[FN240]. See Clarence Morris, The Role of Criminal Statutes in Negligence Actions, 49 Colum. L. Rev. 21, 34 (1949).

[FN241]. See 3 Fowler V. Harper et al., The Law of Torts § 18.6 (2d ed. 1986); Prosser & Keeton, supra note 151, § 56, at 373-77.

[FN242]. See Prosser & Keeton, supra note 151, § 36.221, at n.9; Caroline Forell, The Statutory Duty Action in Tort: A Statutory/Common Law Hybrid, 23 Ind. L. Rev. 781, 782 (1990).

[FN243]. Abdullah v. Am. Airlines, Inc., 181 F.3d 363, 375 (3d Cir. 1999). See also, Donald A. Loose and C. Cyle Brown, The Use of OSHA Regulations in Negligence Cases, 36 Jul. Arizona Attorney 29 (2000).

[FN244]. Hofbauer v. Northwestern Nat'l Bank, 700 F.2d 1197, 1201 (8th Cir. 1983); see also Iconco v. Jensen Const. Co., 622 F.2d 1291, 1296 (8th Cir. 1980).

[FN245]. Hofbauer, 700 F.2d at 1201 (quoting Iconco, 622 F.2d at 1298).

[FN246]. Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 2026 (1996) (codified in 42 U.S.C. 132d-7(a)(2)(B) (2000)).

[FN247]. 29 U.S.C. § 1145 to 1461 (2002).

[FN248]. See United States General Accounting Office, GAO/HEHS-95-167, Employer-Based Health Plans: Issues, Trends, and Challenges Posed by ERISA (1995); Jesselyn Alicia Brown, Note, ERISA and State Health Care Reform: Roadblock or Scapegoat? 13 Yale Law and Policy Review 339, 341 (1995) ("ERISA and State Health Care Reform").

[FN249]. ERISA and State Health Care Reform, supra note 248.

[FN250]. See Nathalie Smith, Note, The Right to Genetic Privacy, 2000 Utah L. Rev. 705, 734 (2000); Rothstein, supra note 52, at 23.

[FN251]. 45 C.F.R. § 164.504(f).

[FN252]. Id.

[FN253]. 45 C.F.R. S164.512(b)(v) (2001).

[FN254]. 479 N.E.2d 113 (Mass. 1985).

[FN255]. 446 S.E.2d 648 (W. Va. 1994).

[FN256]. 45 C.F.R. 164.508(a).

[FN257]. 45 C.F.R. 164.508(b)(4).

[FN258]. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59933 (proposed November 3, 1999).

[FN259]. 65 Fed. Reg. 82475 (December 28, 2000).

[FN260]. Id.

[FN261]. Gostin, supra note 7, at 512.

[FN262]. 45 C.F.R. 164.502(e)(1).

[FN263]. Id.

[FN264]. Restatement (Second) of Agency § 353 (1958).

[FN265]. Bartnicki v. Vopper, 532 U.S. 514 (2001); Fla. Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979); Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978); Okla. Publ'g Co. v. Dist. Ct., 430 U.S. 308 (1977); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975); N.Y. Times v. United States, 403 U.S. 713 (1971).

[FN266]. Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049 (2000).

[FN267]. Michael Frankel, Do Doctors Have a Constitutional Right to Violate Their Patients' Privacy?: Ohio's Physician Disclosure Tort and the First Amendment, 46 Vill. L. Rev. 141, 160-69 (2001); Susan M. Gilles, Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy, 43 Buff. L. Rev. 1, 62-83 (1995).

[FN268]. 532 U.S. 514.

[FN269]. 18 U.S.C. § 2510 to 2521 (1996).

[FN270]. 18 U.S.C. § 2511(1)(a) (1996).

[FN271]. Bartnicki, 531 U.S. at 535.

[FN272]. Bartnicki, 531 U.S. at 526.

[FN273]. Id. at 527 (quoting Daily Mail Publ'g Co., 443 U.S. at 102).

[FN274]. Id. (quoting Daily Mail Publ'g Co., 443 U.S. at 102; Fla. Star, 491 U.S. at 524; Landmark Communications, 435 U.S. at 829).

[FN275]. Id.

[FN276]. Gostin, supra note 7.

[FN277]. The restriction of disclosure of personal information by the government does not raise legal issues under the First Amendment. In fact, with respect to personal health information, the Supreme Court has held that an individual right of privacy exists under the Constitution restricting the ability of governments to collect and disclose such health information. Whalen v. Roe, 429 U.S. 589 (1977); see also United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980).

[FN278]. 435 U.S. 829 (1978). The Court explained, "It can be assumed for purposes of this decision that confidentiality of the (Virginia Judicial) Commission proceedings serves legitimate state interests. The question, however, is whether these interests are sufficient to justify the encroachment on First Amendment guarantees which the imposition of criminal sanctions entails with respect to nonparticipants such as Landmark." Id. at 841 n.12.

[FN279]. 501 U.S. 663 (1991).

[FN280]. Id. at 666-67.

[FN281]. Id. at 672.

[FN282]. See, e.g., Snepp v. U.S., 444 U.S. 507 (1980) (upholding a lower court injunction of the publication of book by CIA officer who had contractually agreed to permit CIA pre-publication review of his materials).

[FN283]. See The Nolan Study, supra note 66.

[FN284]. Nat'l Research Council, For the Record: Protecting Electronic Health Information 40 (1997).

[FN285]. See, e.g., 5 U.S.C. §§ 552a, 482.24; 42 U.S.C. §§ 290dd-3, ee-3 (1988).

END OF DOCUMENT