

Peter A. Winn<sup>1</sup>  
7019 Westlake Ave.  
Dallas, Texas 75214  
[peter.winn@usdoj.gov](mailto:peter.winn@usdoj.gov)  
tel: (214) 659-8684  
fax: (214) 767-2916

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

**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.

---

<sup>1</sup> Adjunct Instructor, Dedman Law School, Southern Methodist University; Assistant U.S. Attorney, U.S. Department of Justice; J.D. Harvard Law School; B.A. Williams College; M.Phil. Philosophy, University College London. 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, Eugene Volokh, Dan Solove, Marc Rotenberg, Peter Swire, Mark Rothstein and Jane Winn.

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<sup>2</sup> (the “HIPAA Privacy Rules” or the “Rules”) became effective, promulgated by the Department of Health and Human Services under the authority of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).<sup>3</sup> 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 disparate functions.<sup>4</sup> Because the increased access to electronic personal health information increases the danger of harmful disclosure and misuse of that information, Congress in HIPAA authorized federal regulatory protections for personal health information.<sup>5</sup> 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

---

<sup>2</sup> 65 Fed. Reg. 82462 (12/28/200), as amended, 65 Fed. Reg. 82944 (12/29/200).

<sup>3</sup> 42 U.S.C.A. § 1320d-2.

<sup>4</sup> See, Final Privacy Rule Preamble, Background and Purpose, Discussion of “Current Law and Practice.” Also see, Confidentiality of Individually Identifiable Health Information, Recommendation of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996 (September 11, 1997).

<sup>5</sup> 42 U.S.C. § 1320d-2(c)(1). 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.

respect to disclosures of their personal health information which were not ordinarily provided under traditional common law doctrines of confidentiality.

The HIPAA Privacy Rules, however, have been criticized for two important perceived shortcomings. First, while the Rules create an administrative enforcement mechanism, they do not create a private cause of action for individuals who are injured by a violation of the Rules. Second, the Rules only subject to legal sanction health care providers, health plans and clearinghouses--what the Rules call "Covered Entities." 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 health care providers and health plans--what the Rules call "Business Associates" of Covered Entities. This has been considered particularly troubling since such Business Associates appear to have been responsible for many of the abuses of personal health information which led to the enactment of the Rules in the first place.

Many leading health care scholars share with the drafters of the Rules a lack of confidence in the ability of the common law to maintain the confidentiality of personal health information in an electronic age.<sup>6</sup> In this article, I argue 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

---

<sup>6</sup> See, 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. 101 (1995); Paul M. Schwartz and Joel R. Reidenberg, Data Privacy Law § 7-3 (1996); For the Record, Protecting Electronic Health Information, National Research Council (1997). But see G. Michael Harvery, *Comment, Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. Pa. L. Rev. 2385 (1992).

private information instead of 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. The invasion of privacy torts tend to be relatively ineffective in addressing the most common types of improper disclosure of health information caused by negligence. However, the breach of confidentiality torts tend to be much more effective in this context—a fact which is not surprising given that the breach of confidentiality tort was originally designed precisely to address the problems of sensitive medical information. I argue 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.

If there is a viable remedy under state law, the first perceived weakness of the Rules--their failure to create a private cause of action--becomes a much less pressing concern. However, the HIPAA Privacy Rules are likely to have complex and interesting relationships with common law doctrines which may produce strong protections for personal health information that neither would be likely to achieve standing alone. For instance, although the HIPAA Privacy Rules create no federal cause of action, an analysis of the case law suggests that the Rules may well be adopted by common law courts to establish a national minimum standard for liability for breach of confidentiality under state law. Just as common law courts traditionally used state statutes and ethical rules to establish a standard of care for breach of confidentiality—even though such statutes and rules rarely provided for a private right of action--the HIPAA Privacy Rules are likely to establish a minimum *federal* standard which will be used in private *state* causes of action for breach of confidentiality.

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.<sup>7</sup> In this context, I review 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. I then compare these common law developments with the 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 Covered Entity. I argue that under the developing case

---

<sup>7</sup> 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 in the Harvard Law Review, 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 though 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.

law, such federally required agreements with Business Associates, while ostensibly creating no liability 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.

The final part of this article addresses the question whether actions for breach of confidentiality applied to Business Associates in a “chain of trust” with a health care provider can survive First Amendment scrutiny. Because they restrict the free flow of information, restrictions on disclosure of information which are designed to protect a “right of privacy” in sensitive personal information have often 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 appear to receive more favorable treatment under standards set out by the Supreme Court in Cohen v. Cowles Media Co.<sup>8</sup> I argue that because tort doctrines such as breach of confidentiality do not create rights of privacy in information because of its personal and sensitive nature, but protect information only in the context of well defined “chains of trust,” they will generally survive First Amendment review.

### **Health Information: Protection and Disclosure**

#### ***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 which no laws

---

<sup>8</sup> 501 U.S. 663 (1991).

against discrimination can banish. Even the disclosure of some medical conditions which 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 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.

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 their 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 their 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.<sup>9</sup> The general rule of confidentiality for medical professionals continues to be strongly emphasized by providers today.<sup>10</sup>

### *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) the first zone involves disclosures which are made between healthcare providers to enable the delivery of primary healthcare; 2) the second zone involves disclosures by providers to payers to ensure the payment of claims and to ensure effective oversight of the payment system, the quality of care provided and for medical research; 3) the third zone involves disclosures which are made to further what are generally deemed socially necessary public purposes, including public health and law enforcement; and 4) the

---

<sup>9</sup> The Hippocratic Oath reads in part as follows:

Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not to be spoken of abroad, I will not divulge as reckoning that all such should be kept secret.

<sup>10</sup> 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). See also, Section M.R. 1.3 of the Manual of The Joint Commission on the Accreditation of Hospitals Standards.

fourth and most controversial zone involves disclosures which take place for private purposes unrelated to treatment and payment.<sup>11</sup>

*Disclosure for Purposes of Treatment*

---

<sup>11</sup> For an excellent discussion of the various forms of disclosure of medical records within the health care industry see, Alan Westin, A Policy Analysis of Citizen Rights Issues in Health Data Systems: Issues in Health Data Systems, ed. Florence Isbell, United States Department of Commerce, National Bureau of Standards (January, 1977), pp. 1-13. This work also contains the earliest analysis of the threat to medical confidentiality created by the computerization of records.

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 and for the training of new physicians.<sup>12</sup> 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, the file may be seen by any nurses, cleaning staff and other hospital personnel on duty in the ward. 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. Within these areas, it is extremely difficult to limit access to patient records only to those individuals actually involved in the treatment of a patient. Hospital stays are also notoriously non-private affairs. The patient usually is scantily clad in a hospital gown, has to share a room with a total stranger, and may be observed semi clad and in various intimate functions by other physicians, nurses, hospital staff, as well as hospital visitors. Paradoxically, this absence of privacy co-exists with a high level of confidentiality. There is a culture among medical professionals and medical staff that sensitive personal information observed in the context of a hospital stay is not disclosed outside of the

---

<sup>12</sup> Hippocratic lore indicates that experienced physicians frequently trained and consulted with less experienced physicians. The use of nurses supervised by more senior medical professionals also dates at least from the time of the early Greeks.

context of the medical treatment arena. Unauthorized disclosures within this first zone of treatment are infrequent, and rarely appear to cause demonstrable harm to patients.

*Disclosure for Payment, Oversight and Research*

a) *Payment*: Historically, when most medical treatment was paid by the individual, through the use of cash, disclosure of medical information outside of the zone of treatment was easily restricted. 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 has become much more widespread.

Standard billing forms within the healthcare industry contain numerical codes listing diagnosis and treatment, as well as much other sensitive personal information about the patient.<sup>13</sup> Merely by virtue of the payment of a health claim, a health plan comes into possession of the single most critical medical information about the patient--the diagnosis and the treatment. 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. Outside experts may be retained by payers to review the claims for medical necessity or the charges for appropriateness within the community.

Disclosure for purposes of payment also takes place when physicians and hospitals hire individuals or outside billing companies to prepare billing forms with appropriate diagnosis and

---

<sup>13</sup> See, e.g., HCFA 1500 forms universally used by physicians, druggists, medical equipment companies and other individual healthcare providers; see also, UB-92 billing forms used by cost reimbursed healthcare providers such as hospitals, nursing homes and home health agencies. Each of these billing forms use ICD9 codes for the diagnosis and CPT codes or DRG codes specifying with great particularity the treatment provided.

treatment codes. Most physicians hire billing and coding personnel to prepare their bills for them, sometimes subcontracting this function to independent billing companies. Hospitals, nursing homes and home health companies may retain independent professionals to review medical records prepared by physicians and nurses and determine codes for 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. Medical equipment companies may contract with billing companies to process claims, and the list goes on.

A health 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.

Furthermore, in spite of the extent of routine disclosure which 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.

b) *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 ensure that the treatment provided was medically necessary and actually delivered. The GAO has estimated that fraud and abuse accounts for 10% of the total United States expenditures on healthcare. Since the United States spends in excess of one trillion dollars per year, 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 investigator, including the notes of the physician, radiological and laboratory reports, drug prescriptions, and other treatment records. At times, physicians may be retained to review medical records or even conduct examinations of patients when suspicions of inappropriate treatment and fraud are being investigated.

In addition to reviews by the private and governmental payers of the bills, the quality of care provided by physicians and other healthcare providers is periodically reviewed by organizations which specialize in utilization review and quality assurance. Utilization review is the system by which hospitals and other medical providers are measured against established norms for use of the facilities, length of stay, patient-staff ratio, and so forth. Quality assurance measures whether the treatment prescribed is appropriate and that the delivery of that care is in conformance with established norms of competence. Many different organizations perform these functions, including the healthcare organizations themselves, health plans and accrediting agencies. Professional licensing authorities review medical records to monitor the quality of care rendered by physicians, nurses, hospitals and other licensed medical providers. These organizations often subcontract with Peer Review Organizations, 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. Typically such reviews may involve the entire patient's medical file. While such oversight also involves risks of improper disclosure, there appears to be a general consensus that some disclosure of sensitive personal health information is critical to appropriate oversight of any properly functioning healthcare system.

Oftentimes the distinction between information processing and the providing of healthcare begins to merge into one another. A pharmacy benefit management company (“PBM”) may be hired by an insurance payer to adjudicate and pay claims as well as manage a formulary. 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 be 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.

Patients may not always be aware of the existence of this vast and complex network of information transfers. A patient who receives marketing materials from what appears to be a drug company with respect to the patient’s medical condition may be rightly 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 has disclosed their confidential prescription information to a drug company for marketing purposes or whether the PBM has merely acted on behalf of the patient’s insurance payer to inform the patient concerning the possible substitution of a lower cost or more effective alternative to the drug prescribed by the physician.

*Research:* Access to medical records is often given to medical researchers to enhance general scientific knowledge or improve treatment protocols. Access to personal medical records for research purposes, particularly at medical schools or within a medical research program, is governed by Institutional Review Boards (“IRB’s”) at the medical institution. While the role of IRB’s is beyond the scope of this article, in general IRB’s are required to have at least

five members, one of whom is from outside the institution. IRB's 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.<sup>14</sup>

*Disclosure for Public Health, Public Safety and Law Enforcement*

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, some of the many instances of such required disclosures are as follows.

Public health officials such as local health departments and such national organizations as the Center for Disease Control, oversee vaccinations, intervene to prevent epidemics, monitor programs to treat pregnant women, intervene with cases of drug addiction and oversee virtually all aspects of the treatment of prisoners. Such bodies are granted broad access to patient health information in the course of executing their responsibilities. State health departments operate in conjunction with law enforcement authorities to track and monitor all prescriptions of certain scheduled drugs to prevent over prescription of addictive drugs and diversion of controlled substances. In the context of civil and criminal litigation, disclosure is often compelled to ensure just adjudication of disputes. Most schools and camps for children require disclosure of vaccinations and other health conditions.

---

<sup>14</sup> See, e.g., Rosnow, Rotheram-Borus, Ceci, Blanck and Koocher, "The Institutional Review Board as a Mirror of Scientific and Ethical Standards," 48 *American Psychologist* 821-826 (1993).

Courts have also found a common law duty to disclose patient information when physicians become aware of such information which, if not disclosed, could result in physical harm or death to members of the public.<sup>15</sup> 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. Several states have enacted partner notification laws when people are diagnosed with AIDS.<sup>16</sup>

While disclosures required as a matter of public policy are sometimes extremely controversial, they 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 public policies served by the required disclosures.

*Private Disclosures Unrelated to Treatment or Payment*

In the private sector, disclosures can take place for purposes unrelated to treatment, payment or health oversight. Two common examples of such private disclosures are in the context of life and health insurance and in the context of employment.

---

<sup>15</sup> See, e.g., Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976).

<sup>16</sup> See, e.g., N.Y. Pub. Health L. § 2130.

*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 other types of insurance. Insurance companies often require potential customers to permit them access to medical records from previous doctors and health care 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 simple physicals conducted by nurses who take simple medical histories and collect blood samples. While insurance companies obtain such information with the consent of the insured, they also engage in the controversial practice of placing health records thus obtained in a central data base called the Medical Information Bureau (“MIB”) where it can be accessed by other insurance companies. The ostensible purpose of such a central database of health records is to prevent insurance fraud.<sup>17</sup> However, any insurance company which is a member of the MIB will have access to large amounts of personal medical information of individuals. While member insurers are officially forbidden from using the information contained in an MIB file as the basis for denying insurance, only as a basis for further investigation,<sup>18</sup> this distinction may not matter to someone whose insurance has been denied based on MIB records. Further, if an MIB member

---

<sup>17</sup> Richard C. Turkington, “Medical Records Confidentiality Law, Scientific Research, and Data Collection in the Information Age,” 24 *Jour. of Law, Medicine & Ethics*, 113, 115 (1997); also see, Simson Garfinkel, “Nobody knows the MIB,” in Database Nation: The Death of Privacy in the 21<sup>st</sup> Century (2000).

<sup>18</sup> Id., at 137.

uses an MIB report of personal health information for purposes unrelated to insurance underwriting (for instance, selling it to a prospective employer), it is difficult to investigate or prosecute such an abuse of the system.

*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 occasional litigation.<sup>19</sup>

---

<sup>19</sup> Young v. Jackson, 572 So.2d 378 (Miss. 1990) (Disclosure by employer to other employees of an employee’s operation for a partial hysterectomy held to be for a legitimate purpose and privileged); Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. App. Ct. 1990) (Disclosure by an employer to other employees of an employee’s mastectomy held to state a cause of action under public disclosure tort.)

The advent of the Employee Retirement Income Security Act of 1976 (“ERISA”), 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. 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. As plan sponsor, an employer is able to review all claims paid by the administration company which necessarily includes specific information concerning diagnosis and treatment. Employers often maintain a company file of all medical insurance claims for each employee at the company. A recent study has found that more than 60% of employers who responded to a poll routinely access employee health information. There is a legitimate concern about the potential for employers to use such information in the context of employment decisions which may have a detrimental impact on an employee’s employment. Access by an employer to such detailed medical information is also extremely problematic for the integrity of the healthcare delivery system, since it has the potential to undermine the relationship of trust between providers and their patients. With respect to this problem, 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.<sup>20</sup>

---

<sup>20</sup> ERISA, sec. 502(a), codified at 29 U.S.C. sec. 1132. See Bobinski, Mary Anne. 1990. *Unhealthy Federalism*, U.C. Davis Law Review 24 (255). See also, Rothstein, Mark A. 1992. *Genetic Discrimination in Employment and the Americans with Disabilities Act*, Houston Law

## **Revolution in Electronic Health Information**

### *Benefits of the Use of Electronic Health Information*

In recent years, more and more health care providers and payers have adopted computerized medical information systems. The use of electronic health information has dramatically improved the quality of treatment which 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. In addition to their greater accessibility, electronic medical records also may be structured in hypertext, permitting relevant information to be expressed with a flexibility impossible with written medical records. The greater accessibility of electronic medical records permits more effective quality assurance; reviewing personnel can quickly determine whether appropriate medical protocols are followed and whether appropriate standards of care are being followed. Review of medical records also can take place by computer programs themselves; 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. While physicians worry about an over reliance on computerized treatment protocols, there is little question than electronic medical records offer significant advantages over paper record keeping systems.

Electronic medical records address the traditional problem caused by the fact that medical treatment typically takes place at different locations, by different physicians with different specialities at different hospitals. The records of such treatments are rarely if ever at a single geographic site. Even routine lab tests and radiological procedures are now performed and interpreted by enterprises located far away from the hospital or doctor which 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. Moreover, the remote access to medical records which is now available permits doctors to check up on their patients from home, or consult with experts in distant parts of the country. Travelers in a remote locale will be treated by doctors who, while they may be strangers, can access the patient's medical record online, and rapidly be able to make a careful and informed diagnosis.

The increasing growth in the use of electronic health information networks has also dramatically accelerated earlier trends in the management and oversight of the payment and treatment process. Computer networks make possible far more extensive efforts by payers to control and manage medical costs. This in turn results in far more extensive requirements for the pre-approval of services, as well as much broader utilization review and quality assurance programs. 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.

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.<sup>21</sup> Likewise, electronic medical records permit public health authorities more effectively to identify, monitor and forecast health threats; more effectively respond and intervene; and evaluate the effectiveness of various public health programs.

*The Problem of the Protection of Electronic Medical Records*

---

<sup>21</sup> The question of conducting genetic research on medical databases raises important legal and ethical concerns when it is not possible for researchers to obtain the consent of all the individuals whose medical records are the subject of the research study. See, generally, Rothstein, *supra*.

Just as the smooth flow of electronic health information provides dramatic benefits, the same smooth flow of electronic health information 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.<sup>22</sup>

This point is not unique to personal health information. In general, the transition from an age in which records were predominately on paper to an age in which records are predominately in electronic form has been accompanied by a lag time in the effective development of effective management structures for the electronic data. The proliferation of the growth in access to electronic information quickly outstrips the procedures which may previously have been in place to control access to the information and otherwise protect it. 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. This tension between the free flow of information and the potential harms from the disclosure of such information exists throughout the field of electronic information.<sup>23</sup>

---

<sup>22</sup> See, Lawrence O. Gostin, *Public Health Law: Power, Duty, Restraint*, 2000, p. 115 for excellent analysis in the context of disclosures with respect to public health.

<sup>23</sup> See generally, Ronald J. Mann & Jane K. Winn, *Electronic Commerce*, ch. 1 (2002); also see Rita C. Summers, *Secure Computing: Threats and Safeguards*, (1997).

As the capacities of hardware, software and communications networks continually increase and the costs of information decrease, information begins to be used in ways which were previously impractical. Much information previously may not have needed protection by legal privacy rules because it retained a high degree of practical privacy because of the inconveniences of retrieving the paper record. A commonly used example is the personal information which was previously stored in public record keeping systems. While this information was technically “public”--that is, it could be accessed by any member of the general public--the process usually required filling out forms, paying fees, and waiting in line for record searches at local, state and federal agencies, courts, department of motor vehicles, deed records offices, electoral commissions, and county records offices. While it was possible to compile a profile of an individual in this manner, doing so was time consuming and costly. Because of the substantial costs of compiling this information, those who typically did access the records had a good reason to do so. Much of this information is now on-line, and a profile can be built of the individual who is a subject of this information in a matter of minutes, at minimal cost.<sup>24</sup> Thus, as more and more information becomes available at lower and lower costs, the free flow of “public” information begins to present an increased risk to privacy which did not present itself in the context of more costly paper records when the cost of accessing this information created a privacy default in practice. This privacy default has now been eliminated and the previous

---

<sup>24</sup> Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Final Version, (June 6, 1995).

public character of the information under the legal regime has become a public default in practice.

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. The information was less useful than its electronic counterpart, but the information benefitted from a default level of protection, simply because it was so hard to get to and very hard to link together into a coherent picture. The same aspects which made for inefficiencies in 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 that person could be held responsible. When personal health information is transformed into an electronic medical record, especially in a networked computer system, the number of people with access to the record dramatically increases and the management of the use of electronic medical information becomes corresponding 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 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 were largely tolerated since they rarely if ever resulted in harm to the patient. 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 which previously accompanied inadvertent disclosures of personal information has begun to erode. 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, as well as the difficulty of proving such access. In an age of electronic medical records, that tolerance has evaporated.

As patients become aware that the world of locked file cabinets in their doctor's 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 raises concerns that patients will begin to adopt strategies of deception or treatment avoidance because of concerns about confidentiality. Concerns of confidentiality may have begun to operate as a practical limit on the potential benefits of electronic medical information.<sup>25</sup> The benefit of the

---

<sup>25</sup> Lawrence Gostin, Privacy and Security of Public Health Information, National Center for Health Statistics. ("The increasing potential for disclosure of this information within a rapidly-developing national health information infrastructure, facilitated by massive computerization of records and other technological developments, presents significant risks to individual privacy."); See also War Stories, Privacy Journal, Robert Ellis Smith.

electronic medical record derives from the fact that electronic information can and does flow freely. If a lack of trust in the integrity of the system causes patients to provide misinformation to health care 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 which may have taken place among medical personnel, or insurance payers, or 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 this trust when electronic medical records are in widespread use. To maintain this trust, the law must carefully balance the need for disclosure of medical information against the need to protect patients from the risk of harm from such disclosure. At stake is the confidence of patients in the medical system itself.

### **The HIPAA Privacy Rules**

The HIPAA Privacy Rules 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.<sup>26</sup> The Rules themselves were the product of a circuitous method devised by Congress when enacting HIPAA<sup>27</sup> to break a legislative deadlock over the issue 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. The

---

<sup>26</sup> See, Gramm-Leach-Bliley Act (also known as Financial Modernization Act of 1999); Children's Online Privacy Protection Act (1998); Telecommunications Act (1996); Driver's Privacy Protection Act (1994).

<sup>27</sup> 42 U.S.C.A. § 1320d-2.

Statute provided, however, 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.<sup>28</sup> When Congress failed to meet its self-imposed deadline, HHS promulgated proposed detailed regulations in November, 1999.<sup>29</sup> The controversial proposed regulations generated over 52,000 comments<sup>30</sup> from nearly every covered entity sector of the affected healthcare payers, providers and clearing houses which were Covered Entities under the Rules. Although comments addressed specific aspects of how the rules affected specific industries, a consistent concern expressed by healthcare providers and payers was that the

---

<sup>28</sup> Id., (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).

<sup>29</sup> 64 Fed. Reg. 59918 (Nov. 3, 1999).

<sup>30</sup> 65 Fed. Reg. at 82566.

proposed Rules would involve extremely high costs to implement.<sup>31</sup> 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, together with a series of other far reaching and controversial labor and environmental regulations.

---

<sup>31</sup> The American Hospital Association has placed a price tag of 43 billion on the Rules.

It was expected that the Rules might be modified by the incoming Bush administration when after taking office in January, the new administration promptly issued a unilateral order rescinding the entire corpus of Clinton's "midnight" regulatory onslaught.<sup>32</sup> Although the HIPAA Privacy Rules were not covered by the order, both the rules' proponents as well as opponents expected that a Bush administration generally sympathetic to business and suspicious of costly governmental regulations would make significant revisions to the regulations in order to lessen their costs to the healthcare industry.<sup>33</sup> This expectation was confirmed when on February 23, 2001, faced 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 30-day public comment period.<sup>34</sup> As more than 24,000 additional comments

---

<sup>32</sup> [http://www.whitehouse.gov/omb/inforeg/regreview\\_plan.pdf](http://www.whitehouse.gov/omb/inforeg/regreview_plan.pdf). The order imposed a moratorium on all regulations that were published in the Federal Register but were not yet final. However, the order specifically exempted from the moratorium regulations promulgated pursuant to a statutory or judicial deadline. The federal health privacy regulations were not covered by the moratorium, since they were promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA specifically required the regulation be promulgated in final form no later than 42 months after the enactment of HIPAA.

<sup>33</sup> In the face of a strong April 9, 2001 attack on the HIPAA Privacy Rules by House Majority Leader Dick Armey, (<http://www.freedom.gov/library/technology/memo/privacy.asp>.) the Health Privacy Project's announcements were mournful. ("Between today and April 14, 2001, we expect that Secretary Thompson of the U.S. Department of Health and Human Services (HHS) will take action to delay and/or change the final medical privacy regulation." Health Privacy Project: Status of Federal Health Privacy Regulation, April 9, 2001 ([http://www.healthprivacy.org/info-url\\_nocat2303/info-url\\_nocat\\_show.htm?doc\\_id=55491](http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=55491).) On the other hand, the American Hospital Association sounded confident. ("The medical privacy rule in its current form is unworkable for hospitals and their patients and represents one of the largest unfunded federal mandates in recent memory. According to a study commissioned by the AHA, the costs of only three narrow provisions of the rule could exceed \$22 billion over five years for hospitals." (<http://www.aha.org/ar/Comment/letters.asp?lookupLetterID=229>.)

<sup>34</sup> The request for public comments was published in the Federal Register (66 Fed. Reg.

arrived, Secretary Thompson publicly forecasted that HHS would make significant changes in the rules to lessen the financial burden on the healthcare industry.<sup>35</sup> Instead, something else happened. On April 12, 2001, in a surprising turn of events, less than two weeks after the close of the newly opened comment period, the Bush administration announced that the HIPAA Privacy Rules would go into effect as originally promulgated by the Clinton administration. The additional comments were dismissed as “cumulative” and, while acknowledging that some minor modifications might be permitted, the Administration sent strong signals that it was not inclined to permit significant modifications in the future. Bush was now espousing pro-privacy rhetoric virtually indistinguishable from that used by the previous Democratic administration and was advertising himself as “the privacy president.”<sup>36</sup>

---

12738). The announcement stated, "The department will review the comments it receives to determine whether changes in the final rule are needed."

<sup>35</sup> On March 27, 2001, Secretary Thompson told reporters, "I am fairly certain, without saying for sure, there will be some modifications to simplify and to lessen the financial burden." (Reuters Health, 3/28/01)

<sup>36</sup> <http://www.hhs.gov/news/press/2001pres/20010412.html>. The only modifications which were indicated were to eliminate confusion in the final regulations regarding necessity of consent forms for access by other healthcare providers such as consulting physicians and pharmacists and clarifying the right of parents to gain access to their children’s medical records.

---

Compare the Clinton administration's announcement at:  
<http://www.hhs.gov/news/press/2000pres/20001220.html>.

Most health plans and healthcare providers that are covered by the Rule must comply with the Rule's requirements by April 14, 2003, or two years from the effective date of the Rule; small health plans have until April 14, 2004. The Rules themselves face legal challenges<sup>37</sup> as well as Congressional attempts to replace them with less stringent legislation. However, what appears to have emerged from the political drama is significant bi-partisan agreement between diverse political factions that a pressing need exists for national standards to protect individually identifiable health information, even if it involves significant costs to the healthcare industry.<sup>38</sup> As the April 14, 2003 compliance date approaches, most healthcare providers and payers have resigned themselves to begin a significant effort to comply with the new Rules.<sup>39</sup>

---

<sup>37</sup> See South Carolina Medical Association, et al. v. U.S. Dept. of Health and Human Services, et al., No. 3:01-2965-19 (District Court, Columbia, South Carolina), Complaint for Declaratory Relief filed July 31, 2001. The Society of American Physicians and Surgeons have announced they intend to file suit against the HIPAA Privacy Rules in U.S. District Court in Houston, Texas.

<sup>38</sup> While the administration has agreed to delay implementation of other provisions of HIPAA, including the administrative simplification provisions, the administration has indicated that the compliance deadline for the HIPAA Privacy Rules will not be delayed.

<sup>39</sup> Due to a technical omission in the publication of the final rule, the rule's effective date was moved to April 14, 2001. As a result the compliance dates also changed to two years after the effective date.

### Overview of the Rules

The HIPAA Privacy Rules were issued in the context of the “Administrative Simplification” provisions of HIPAA which authorized 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.<sup>40</sup> 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. 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, the HIPAA Privacy Rules establish detailed nationwide minimum<sup>41</sup> standards for the protection of what it terms “individually identifiable health information.”<sup>42</sup>

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

---

<sup>40</sup> 42 U.S.C. § 1320d-2 et seq.

<sup>41</sup> The Rules in fact only establish a federal floor of protection and do not pre-empt any state standards which provide greater protection than do the Rules. Congress, faced with widespread interstate access to new forms of electronic healthcare information, directed HHS to establish minimum standards to protect such electronic health information.

<sup>42</sup> While payers and providers may still be subject to higher state confidentiality requirements, it is unclear how effective higher state standards will be for interstate electronic

of protection for personal medical information. 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 other reasons 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.

#### Covered Entities Under the Rules

HIPAA Section 1173(a)(1) limits the application of the proposed rule to 1) health plans, 2) healthcare clearinghouses, and 3) healthcare providers. A *healthcare provider* is anyone who furnishes, bills or is paid for healthcare in the normal course of business. This includes doctors, nurses, therapists and medical technicians. It includes hospitals, pharmacists, nursing homes, home health companies, medical equipment providers and research institutes. 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. It also includes Health Maintenance Organizations. 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. Finally the

---

information.

term *healthcare clearinghouses* includes, billing companies and organizations like the Medical Information Bureau discussed above which aggregate health information.

Covered Entities are required under the Rules to implement compliance programs to ensure that the confidentiality requirements of the Rules are followed. 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. The Rules also require the designation of a “privacy official,” i.e., an employee responsible for developing and implementing these policies.

#### *Individually Identifiable Health Information*

The HIPAA Privacy Rules apply to all individually identifiable health information (“IIHI”) which 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.<sup>43</sup> IIHI is defined as information which is created or received by a healthcare provider, health plan or clearing house which 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 which identifies the individual or could be used to identify the individual.<sup>44</sup> The Rules allow for the option of de-Identifying IIHI prior to its disclosure to third parties.<sup>45</sup> However, given the unique nature of diagnosis and treatment codes, it is virtually impossible to ensure that information which retains diagnosis and treatment

---

<sup>43</sup> 45 C.F.R. § 164.501.

<sup>44</sup> 45 C.F.R. § 164.501.

<sup>45</sup> 45 C.F.R. § 164.514(b)(2)(i).

codes will not be individually identifiable. Most medical providers have not engaged in serious attempts to render their medical information anonymous.

### Consents and Authorizations

The Rules create two categories of consents permitting disclosure: Consents and Authorizations. Healthcare providers “with a direct treatment relationship” must obtain consent to use personal health information for treatment, payment or healthcare operations.<sup>46</sup> Such consent forms, however, are largely ritualistic, since the provider may condition treatment on the execution by a patient of a form consenting to disclosure. In addition, within this routine form of consent, providers may disclose personal health information for purposes of public health reporting, for purposes of reporting child abuse or neglect or other abuse, neglect or domestic violence, to report communicable diseases, for health oversight activities, for purposes of judicial and administrative proceedings, law enforcement purposes, for purposes of identifying deceased persons, to avert a serious threat to public health or safety, for research (subject to the approval of a privacy board and subject to other specific criteria) and other specific governmental functions.<sup>47</sup> This list of permitted disclosures is very similar to the list of permitted disclosures under common law confidentiality standards. Thus, in general, the HIPAA Privacy Rules allow for the smooth flow of identifiable health information for treatment, payment, and related operations, as well as for the traditional purposes permitted and required under state and federal disclosure laws.

---

<sup>46</sup> 45 C.F.R. § 164.506.

<sup>47</sup> 45 C.F.R. § 164.512(a)-(k).

For any other disclosures, a formal authorization must be obtained from the individual who is the subject of the information. This 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. 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 that authorization from the individual. In addition, the Rules require individual authorization for use and disclosure of psychotherapy notes in most circumstances. Finally, a covered entity may not condition an individual’s treatment, payment, enrollment, or eligibility on the provision of an authorization. The authorization may be later revoked by the individual.<sup>48</sup>

---

<sup>48</sup> 45 C.F.R. § 164.508(b)(4).

The Rules' strict requirements with respect to "authorization" forms are intended to address abuses of broad consent or authorization forms. These broad consent forms have become a standard part of visits to doctors, hospitals and other healthcare providers. While most reputable healthcare providers limit the language on such forms to disclosures for treatment and payment, unscrupulous providers, and insurance companies, have sometimes used the broad authorizations for disclosure of medical information, for purposes entirely unrelated to treatment and payment decisions. Since such forms lack any meaningful notion of consent—patients being presented with the forms at a time when they are least likely to risk not receiving healthcare services—the general release forms have been aptly called by Professor Turkington "the black hole" of confidentiality.<sup>49</sup> The Rules largely eliminate these abusive practices. The overall effect is that other than for these listed purposes, the Rules prohibit the flow of identifiable information for any additional purposes unless specifically and voluntarily authorized by the subject of the information.

*Minimum Necessary Disclosure Standard*

---

<sup>49</sup> See Richard Turkington, "Medical Records Confidentiality Law, Scientific Research, and Data Collection in the Information Age, 24 Jour. Of Law, Medicine & Ethics, 113, 119 (1997).

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 the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”<sup>50</sup> The Rules permit Covered Entities flexibility in the determination of what constitutes “reasonable efforts.”<sup>51</sup> The guidelines issued by the Secretary also make it clear that this provision allows for a broad range of reasonableness as to what “minimum necessary” means for each provider. While the minimum necessary requirement would appear to end the widespread system of disclosures discussed above, the Rules contain general limitation that they do not prohibit disclosures “otherwise required by law.” As we have seen, disclosures ordinarily takes place pursuant to statutes or regulations or case law. Accordingly, the Rules leave the system of widespread disclosure of medical information largely unaffected, in effect codifying the pragmatic balance previously in place under the system of protection and disclosure which existed under state law before the Rules.

#### *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. The concept of fair information practices developed in the late 1960's and early 1970 by scholars such as Alan Westin<sup>52</sup> and Arthur

---

<sup>50</sup> 45 C.F.R. § 164.502(b)(1).

<sup>51</sup> 65 Fed. Reg. at 82,714 (noting that the final regulations do not require “all reasonable efforts” as required by the proposed regulations).

<sup>52</sup> Alan F. Westin and Michael A. Baker, Databanks in a Free Society: Computers, Recordkeeping and Privacy 229 (1972). See also, Alan F. Westin, Privacy and Freedom, (1967).

Miller<sup>53</sup> who were concerned with the implications of widespread conglomerations of personal information in computerized databases. In 1973, a path breaking report by the Department of Health, Education and Welfare entitled Records, Computers and the Rights of Citizens<sup>54</sup> (the "HEW Report"), addressed certain fundamental concerns involved with the use of electronic information to collect, access and store information about individuals. To address these concerns, the HEW Report articulated the following set of general principles entitled a "Code of

---

<sup>53</sup> Arthur R. Miller, Computers, Data Banks and Individual Privacy: An Overview, 4 Colum. Humna Rights L. Rev. 1, 1-10 (1972).

<sup>54</sup> U.S. Department of Health, Education, and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973) ("HEW Report").

Fair Information Practices.” 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.<sup>55</sup> Various aspects of fair information practices have been incorporated into numerous federal statutes, including, the Privacy Act of 1974, the Family Educational Rights and Privacy Act of 1974, and the Video Privacy Protection Act of 1988, as well as many similar state statutory privacy protection schemes. In Europe, the American designed fair information practices have been formally adopted by the European Community in the form of the privacy directive.<sup>56</sup>

---

<sup>55</sup> Id. The relevant provisions of the Code of Fair Information Practices read 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.

<sup>56</sup> See Council of Europe, Convention for the Protection of Individuals with Regard to

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.<sup>57</sup> Patients have the right to inspect and copy their own personal health information.<sup>58</sup> They have the right to request amendments of erroneous or incomplete information.<sup>59</sup> They have the right to obtain an accounting of any disclosures of their information for any purposes other than treatment and payment.<sup>60</sup> They have the right to file complaints if they believe the covered entity has not followed its privacy policies.<sup>61</sup> The Rules require persons who hold identifiable health information to safeguard that information from inappropriate use or disclosure, and Covered

---

Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108; O.E.C.D., 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 final (1980).

<sup>57</sup> 45 C.F.R. § 164.520.

<sup>58</sup> 45 C.F.R. § 164.524.

<sup>59</sup> 45 C.F.R. § 164.526(a).

<sup>60</sup> 45 C.F.R. § 164.528(a).

<sup>61</sup> 45 C.F.R. § 164.530(d).

Entities must implement safeguards to protect health information from intentional or accidental misuse.

### *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 which provide services or a product which involves the transfer of individually identifiable medical information. Business Associates include third party administrators, some billing firms, pharmacy benefit management companies, disease management firms, companies which provide utilization review, companies which provide management or quality assurance services and companies which perform data processing operations for health plans and healthcare providers. Business Associates also include lawyers and accountants who work for healthcare providers and health plans. 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 health care 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 Associates agree to abide by the same requirements to safeguard health information as the Covered Entities.<sup>62</sup> Since all personal health information derives ultimately from healthcare providers

---

<sup>62</sup> 45 C.F.R. § 164.504(e).

who are in turn under a duty of confidentiality with the individual patient, what this provision of the Rules effectively does is put Business Associates under a contractual obligation that effectively makes them agents of the Covered Entities with respect to their use of personal health information. As such they are placed under the same duty of confidentiality with respect to the personal health information as the covered entity.<sup>63</sup> 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.<sup>64</sup>

#### Enforcement of the Rules

The Rules are enforced through criminal and administrative penalties. Administratively, HHS Secretary has the authority to impose civil monetary penalties against Covered Entities which fail to comply with the requirements of the rule. The fines the secretary is permitted to levy are limited to \$25,000 for each calendar year for each provision which is violated.<sup>65</sup> 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 10 years and substantial fines if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain.<sup>66</sup> These sanctions, however, apply only to the Covered Entities. There are no criminal or administrative remedies which apply to Business Associates which misuse personal health information. While Covered Entities must take "reasonable steps"

---

<sup>63</sup> Cite

<sup>64</sup> 45 C.F.R. § 164.504(e)(2).

<sup>65</sup> 42 U.S.C. § 1320d-5.

<sup>66</sup> 42 U.S.C. § 1320d-6.

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.

### **Breach of Confidentiality under the Common Law**

The Preamble to the HIPAA Privacy Rules give as a chief reason for the need of federal protections for personal health information the lack of significant protections for the privacy of medical records under state common law and statutes. In fact, in the following discussion, I argue 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 which 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.<sup>67</sup> I argue that the Rules will interact with Common Law doctrines to fill in these legal gaps.

---

<sup>67</sup> the original proposed Rules provided that the contracts between Covered Entities and Business Associates must ensure that patients whose personal information was transferred to a Business Associate were to be expressly identified as “third party beneficiaries” of the contract. However, the “third party beneficiary” requirement was extremely controversial and was withdrawn from the final Rules.

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 of personal health information.<sup>68</sup> 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 which will not occur in most cases involving the release of health information.<sup>69</sup> Another restriction of the public disclosure tort is

---

<sup>68</sup> The Restatement (Second) of the Law of Torts summarizes the types of situations in which a cause of action for invasion of privacy arises.

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye, and
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

<sup>69</sup> Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976). For criticisms of the requirement of widespread publication, see Miller v. Motorola, 202 Ill. App. 3d 976, 560 N.E.2d 900, 902 (1990). See also Keeton, W. Page (ed.) 1984. Prosser and Keeton on the Law of Torts. Sec. 117, at 857-858.

that most courts define disclosure as the release of information to someone without a legitimate interest in the information.<sup>70</sup> As we have seen, 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, and that the disclosure to strangers--who have no interest in the information at all--often poses a marginal threat. Finally, and most importantly, the invasion of privacy torts require the plaintiff to show an intentional disclosure, while most disclosures of sensitive health information happen by accident.

Many scholars, while noting that invasion of privacy has different legal elements from breach of confidentiality, assert that the two torts serve fundamentally the same purposes. I believe 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 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. 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 implies the failure of breach of confidentiality theories. If the “invasion of privacy” torts do not protect personal health information, it may be that they were never designed to do so. On the other hand, the tort of breach of confidentiality originated

---

<sup>70</sup> Id.

in the context of health care and was designed with the problems of protecting health information specifically in mind.

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.<sup>71</sup> 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 which 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, as well as

---

<sup>71</sup> See, e.g., Hammonds v. Aetna Cas. & Sur. Co., 243 F.Supp. 793 (N.D. Ohio 1965); Horne v. Patton, 291 Ala. 701, 287 So.2d 824 (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, 395 Mass. 59, 479 N.E.2d 113 (1985), cert. denied, 474 U.S. 1013, 106 S.Ct. 546, 88 L.Ed.2d 475 (1985); Saur v. Probes, 190 Mich.App. 636, 476 N.W.2d 496 (1991); Brandt v. Medical Defense Assocs., 856 S.W.2d 667 (Mo. 1993) (en banc); Simonsen v. Swenson, 104 Neb. 224, 177 N.W. 831 (1920); Hague v. Williams, 37 N.J. 328, 181 A.2d 345 (1962); Estate of Behringer v. Medical Ctr. at Princeton, 249 N.J. Super. 597, 592 A.2d 1251 (Law Div. 1991); MacDonald v. Clinger, 84 A.D.2d 482, 446 N.Y.S.2d 801 (N.Y. App. Div. 1982); Humphers v. First Interstate Bank, 298 Or. 706, 696 P.2d 527 (1985) (en banc); Schaffer v. Spicer, 88 S.D. 36, 215 N.W.2d 134 (1974); Berry v. Moench, 8 Utah 2d 191, 331 P.2d 814 (1958); Morris v. Consolidation Coal Co., 191 W.Va. 426, 446 S.E.2d 648 (1994); McCormick v. England, 328 S.C. 627, 494 S.E.2d 431 (1998). Only Tennessee has not expressly permitted recovery for a physician's breach of the duty of confidentiality, Quarles v. Sutherland, 215 Tenn. 651, 389 S.W.2d 249 (1965), but cases acknowledge the existence of the duty of confidentiality. 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).

common law principles of trust, and the Hippocratic Oath and principles of medical ethics which prohibit the revelation of patient confidences.<sup>72</sup>

One of the earliest cases discussing the liability of a physician for disclosure of patient information is Simonsen v. Swenson,<sup>73</sup> a case in which a physician had treated a patient while the patient was staying in a hotel. 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. 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. 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.

---

<sup>72</sup> Alberts v. Devine, 395 Mass. 59, 479 N.E.2d 113, 119 (1985), cert. denied, 474 U.S. 1013, 106 S.Ct. 546, 88 L.Ed.2d 475 (1985)

<sup>73</sup> 177 N.W. 831 (Neb. 1920).

Virtually all subsequent cases finding a common law tort of breach of confidentiality rely on statutes and ethical rules which, while not providing a individual cause of action for their violation, are used to establish the standard of care which is alleged to have been violated. In Horne v. Patton,<sup>74</sup> Horne's physician disclosed information to his employer, contrary to his express instructions. Horne alleged that the doctor-patient relationship was a confidential relationship which created a fiduciary duty by the doctor, that the unauthorized release of information breached the fiduciary duty, and further, that it violated the Hippocratic Oath, constituting unprofessional conduct. The Supreme Court of Alabama held there was a confidential relationship between a physician and patient which imposed a duty upon the physician not to disclose information concerning the patient obtained in the course of treatment. 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. 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[.]"<sup>75</sup>

---

<sup>74</sup> 291 Ala. 701, 287 So.2d 824 (1973).

<sup>75</sup> Id. at 829.

Likewise, in Hague v. Williams,<sup>76</sup> 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.<sup>77</sup> The court observed that it was not concerned with the physician-patient privilege because "it deals with testimony in a judicial proceeding."<sup>78</sup> The court explained the importance of the physician-patient duty of confidentiality: "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." *Id.* at 349. Likewise, in Humphers v. First Interstate Bank,<sup>79</sup> the Supreme Court of Oregon held that the actionable wrong was the breach of the duty arising from a confidential relationship. 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." The Court did not ground its decision on the statute, but upon the common law duty which was breached by the defendant.

As Alan B. Vickery, expresses it, "[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.

---

<sup>76</sup> 37 N.J. 328, 181 A.2d 345 (1962).

<sup>77</sup> *Id.* at 349.

<sup>78</sup> *Id.* at 348.

<sup>79</sup> 298 Or. 706, 696 P.2d 527, 535 (1985) (en banc).

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."<sup>80</sup>

---

<sup>80</sup> Alan B. Vickery, Note, Breach of Confidence: An Emerging Tort, *supra*, at 1451.

Courts have sometimes described the breach of confidentiality tort as based on invasion of privacy, breach of an implied term of a contract, and breach of the fiduciary relationship.<sup>81</sup> It is accurate to describe a breach of confidentiality as a breach of an implied term of a contract and the breach of a fiduciary relationship. However, while the concept of privacy is sometimes mentioned in breach of confidentiality decisions, the tort is quite different from an invasion of privacy.

---

<sup>81</sup> See, e.g., Alberts v. Devine, 395 Mass. 59, 479 N.E. 2d 113, cert. denied, 474 U.S. 1013 (1985); MacDonald v. Clinger, 84 A.D.2d 482, 446 N.Y.S.2d 801 (1982). Horne v. Patton, Ala.Supr., 287 So.2d 824 (1973); Vassiliades v. Garfinckel's, Brooks Bros., D.C.App., 492 A.2d 580 (1985); Leger v. Spurlock, 589 So.2d 40 (1991); Alberts v. Devine, 479 N.E.2d 113 (1985); Hague v. Williams, 181 A.2d 345 (1962); Behringer Est. v. Princeton Med. Ctr., 592 A.2d 1251 (1991); Humphers v. First Interstate Bank, 696 P.2d 527 (1985); Berry v. Moench, 331 P.2d 814 (1958). Also generally, see Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 Columbia L. Rev. 1426 (1982).

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.<sup>82</sup> 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. 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. On the other hand, the right of privacy does not cover such a case.<sup>83</sup>

Second, in a breach of confidence case, the information is protected without regard to the degree of its offensiveness to a reasonable person.<sup>84</sup> To establish a claim for invasion of privacy, the disclosure must be highly offensive to a reasonable person. If 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.

Third, the disclosure of the information need not be intentional.<sup>85</sup> Under the classic common law invasion of privacy torts, the conduct complained of must be intentional while

---

<sup>82</sup> Rycroft v. Gaddy, 281 S.C. 119, 314 S.E.2d 39 (Ct.App.1984). See also Swinton Creek Nursery v. Edisto Farm Credit, 326 S.C. 426, 483 S.E.2d 789 (Ct.App.1997) (a communication to an individual or even a small group does not give rise to liability unless there is some breach of contract, trust, or confidential relationship which will afford an independent basis for relief).

<sup>83</sup> Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, *supra*, at 1442.

<sup>84</sup> See McCormick v. England, *supra*, 640-641 for comparison to invasion of privacy tort.

<sup>85</sup> Id.

breach of confidentiality by a physician can be unintentional or accidental, and can be established merely upon a showing of failure to take reasonable care to protect the sensitive health information.

Fourth, there is no defense that the facts disclosed are of great public interest,<sup>86</sup> the disclosure must have been intentional, the facts revealed must be of no legitimate public interest and the disclosure must be highly offensive to a person of ordinary sensibilities. Privacy is a right against the public at large. However, because of the broadness of the tort, it is very narrowly circumscribed in its doctrinal limits. 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. In contrast, a right to confidentiality exists 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.<sup>87</sup>

The invasion of privacy tort protects the right of an individual to “be left alone.” It does not presuppose disclosure, but presupposes the right to control the disclosure of information. By contrast, the breach of confidentiality tort presupposes that the appropriate state of affairs is the disclosure of information, albeit restricted, in the relationship with a physician. The tort is intended to secure the integrity of the relationship between the provider and the patient. As

---

<sup>86</sup> See Alan B. Vickery, Note, Breach of Confidence: An Emerging Tort, *supra*, at 1441.

<sup>87</sup> McCormick v. England, *supra*, 640, citing Alan B. Vickery, Note, *supra*.

such, the tort presupposes disclosure in the context of a professional relationship between physician and patient.

This relationship extends beyond the concept of contract. For instance, if the matter were purely one of contract law, a patient should be able to consent to any third party disclosure by the physician. In fact, the physician, like an attorney, is limited by the professional ethics of the relationship from entering into such a contract. Under current ethical rules applying to physicians, the patient's consent may not be effective to relieve a physician of liability for a disclosure which harms the patient. Just as a client could not consent to disclosure of future privileged communications with an attorney in exchange for a reduced hourly rate, so too a patient's consent to broad downstream disclosure would not shield a doctor from liability if this disclosure could be foreseen to cause harm to the patient. This is easiest to see in the case of psychiatric care, but it is not restricted to that profession. Instead, the professional ethical rules governing the professional relationship place a fiduciary duty on the physician with respect to the patient's personal medical information. Just as the patient cannot authorize complete disclosure of their personal health information, the patient does not have unfettered right to refuse to consent to any secondary disclosure. As a fiduciary the physician may have to consult with another physician, such as a specialist, when he believes that such consultation may be necessary for the health of the patient. Ideally, such secondary disclosures would take place with the patient's knowledge and consent, but the law does not impose liability if the physician makes such consultations against the wishes of the patient and without the knowledge of the patient.

**Justified Disclosures not a Breach of Confidentiality**

When health information is disclosed in a manner which causes harm to the patient there is a presumptive cause of action for breach of confidentiality. However, there are a broad range of contexts in which the disclosure of health information by a medical professional is justified. In these instances, the disclosure is not actionable. We have already examined Simonsen v. Swenson,<sup>88</sup> the very earliest American common law case involving breach of confidentiality which in fact found the physician's disclosure was justified and privileged. In general, these cases permit disclosures on the basis of pragmatic balancing tests, with an expectation that there continues to be a duty on the part of downstream entities to maintain the confidentiality of the information against further disclosure.

---

<sup>88</sup> 177 N.W. 831 (Neb. 1920).

Under the common law and most state statutes, disclosure is permitted or sometimes even required when the public interest in disclosing the confidence outweighs the duty to keep it confidential. For instance, public policy requires that where it is reasonably necessary to protect the interest of the patient or others, a physician may sometimes disclose confidential patient information without incurring liability for breach of confidentiality.<sup>89</sup> Statutes and regulations require the sharing of personal medical information for public health purposes, third party

---

<sup>89</sup> 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 a purpose...." Berry v. Moench, 8 Utah 2d 191, 331 P.2d 814, 817-18 (1958). See also Mull v. String, 448 So.2d 952 (Ala.1984) (disclosure of patient information allowed when patient's health is at issue in litigation); Simonsen v. Swenson, 104 Neb. 224, 177 N.W. 831 (1920) (disclosure of information about a highly contagious disease is privileged and not a breach of the duty of confidentiality). In Saur v. Probes, 190 Mich.App. 636, 476 N.W.2d 496, 499-500 (1991), 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." In Estate of Behringer v. Medical Center at Princeton, 249 N.J.Super. 597, 592 A.2d 1251, 1268-69 (Law Div.1991), the New Jersey court discussed a variety of exceptions to the duty of confidentiality.

payment, fraud investigations and other reasons such as judicial and administrative proceedings, by law enforcement, and in emergency circumstances.

In the famous case of Tarasoff v. Regents of University of California,<sup>90</sup> 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. 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. Most states have statutes requiring disclosure by a physician of suspected physical or mental abuse of a child or an elderly or mentally disabled person. Likewise, many states require physicians to notify a spouse or known contact of a person having HIV infection or AIDS.<sup>91</sup> All states which place an affirmative duty of disclosure on physicians either expressly or impliedly provide a grant of immunity from liability for breach of confidentiality for such disclosures.<sup>92</sup> Thus, the breach of confidence tort evidences a pragmatic and utilitarian balancing which permits disclosures of medical information when these disclosures serve a legitimate purpose and when the public benefit of disclosure or danger from non-disclosure outweighs the harm inflicted on the relationship of trust between patient and physician.

---

<sup>90</sup> 17 Cal.3d 425, 551 P.2d 334, 131 Cal. Rptr. 14 (1976).

<sup>91</sup> S.C.Code Ann. S 44-29-146 (Supp.1996).

<sup>92</sup> See, e.g., S.C.Code Ann. S 20-7-510 (Supp.1996); S.C.Code Ann. S 20-7-540 (Supp.1996); S.C.Code Ann. S 20-7-550 (Supp.1996).

A example of balancing under the common law is the case of Behringer v. Medical Center at Princeton.<sup>93</sup> 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. 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. 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. 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. The court held that the design and management of a health records system is a duty which requires a medical provider to balance the possible harm from unauthorized disclosure against the cost of reducing the risk of disclosure.

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. The Behringer case is on point. The system which had been implemented by the hospital to prevent misuse of information was designed to protect

---

<sup>93</sup> 249 N.J. Super. 597, 592 A.2d 1251 (Sup. Ct. 1991)

information from outsiders. When the subject of the AID's 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. As a practical matter, 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 which causes significant harm to 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.

#### **Downstream Third Party Liability for Breach of Confidentiality**

As we have seen, because the breach of confidence tort requires the existence of a special kind of relationship, it has been considered ineffective when the relationship is absent. Traditionally, it has been difficult to establish fiduciary liability for third parties who are downstream in the information flow. If confidential medical information is passed from a physician to a an insurer, does the insurer holding the medical information also have a duty to maintain the confidentiality of the information? The answer provided by at least some common law courts is yes. The breach of confidence can be committed not only by a provider, but by a payer, such as an insurance company.

The earliest case of this case was Hammonds v. Aetna Casualty & Surety Company,<sup>94</sup> in which the physician of Hammonds, who was in personal injury litigation with an insurance company was also covered by malpractice insurance by the same insurance company. The

---

<sup>94</sup> 343 F.Supp. 793 (N.D. Ohio, 1965).

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. Hammonds brought suit against the insurance company for inducing the physician to divulge confidential information gained through a physician-patient relationship. The physician was also a nominal defendant, but the complaint only accused the physician of misfeasance predicated on misinformation and directed its plea for redress solely against the insurance company. Hammonds' theory of the case was that one who induces a physician's treachery may also be held liable for damages. The court held that when one induces a doctor to divulge confidential information in violation of the doctor's legal responsibility to his patient, the third party may also be held liable in damages to the plaintiff. The courts in Ohio do not restrict this holding to insurance carriers who obtain confidential information from physicians through the use of pretexts.

In Alberts v. Devine,<sup>95</sup> 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. 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 which must be present in order to establish liability for inducing a fiduciary to breach his fiduciary relationship:

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

---

<sup>95</sup> 395 Mass. 59, 479 N.E.2d 113 Mass. (1985).

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.<sup>96</sup>

---

<sup>96</sup> Alberts, 479 N.E.2d at 121 (citations omitted).

Alberts was followed in Morris v. Consolidation Coal Co.<sup>97</sup> In that case, the Supreme Court of Appeals of West Virginia found liability not only against the physician, but the third party as well. Morris also involved a disclosure of confidential medical information by a physician to an employer in the context of a workmen's compensation dispute. 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, finding in the affirmative.<sup>98</sup>

Very recently, in the case of Biddle v. Warren General Hospital,<sup>99</sup> the Ohio Supreme Court held that a law firm representing a hospital was liable for inducing a hospital to breach patient confidentiality. 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 Social Security Insurance Disability benefits ("SSDI"). If the patients were found eligible for SSDI, Medicare would pay their hospital bills. It was expected that the law firm would provide legal representation to some of these patients in attempting to get SSDI benefits. While the Court recognized the need in some contexts for an attorney representing a healthcare provider to review personal medical information, permitted the law firm to review virtually every patient file in the hospital was found not to be reasonable. 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

---

<sup>97</sup> 191 W.Va. 426, 446 S.E.2d 648 W.Va. (1994).

<sup>98</sup> The Court cites Hammonds, 243 F.Supp. at 803; Alberts v. Devine, 395 Mass. 59, 479 N.E.2d 113, 121 (1985), cert. denied, Carroll v. Alberts, 474 U.S. 1013, 106 S.Ct. 546, 88 L.Ed.2d 475 (1985); and Anker v. Brodnitz, 98 Misc.2d 148, 413 N.Y.S.2d 582 N.Y.Sup. (1979).

accessing the patient records for the benefit of the hospital or so the law firm could attract new clients.

The general rule 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 confidentiality that the physician owed the patient; and (4) the physician wrongfully divulges confidential information to the third party.

#### **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 scope of the government's ability to bring enforcement proceedings under the Rules is limited to Covered Entities. 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 pre-empt state confidentiality laws which

---

<sup>99</sup> 86 Ohio St.3d 395, 715 N.E.2d 518 (1999)

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, however, is whether the Rules will be adopted by state courts adjudicating state common law breach of confidentiality claims. This question almost certainly appears to be answered in the affirmative.

In Cort v. Ash,<sup>100</sup> the Supreme Court enunciated the following four-part test for implying a private cause of action for the violation of a federal statute: 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 States, so that it would be inappropriate to infer a cause of action based solely on federal law?<sup>101</sup> In more recent cases the Supreme Court has looked almost exclusively to congressional intent--the Cort v. Ash criteria being treated as indicia of that intent.<sup>102</sup> Since

---

<sup>100</sup> 422 U.S. 66 (1975).

<sup>101</sup> *Id.* at 78, 95 S.Ct. at 2088 (citations omitted).

<sup>102</sup> Transamerica Mortgage Advisors, Inc. v. Lewis, 444 U.S. 11, 100 S.Ct. 242, 62

deciding Cort v. Ash the Court has become increasingly more reluctant to imply new private causes of action for damages.<sup>103</sup> Given the provision of both criminal and administrative remedy 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 HIPAA Privacy Rules. However, it does not follow that the HIPAA Rules will not become the basis of a private cause of action under state law.

---

L.Ed.2d 146 (1979); Touche Ross & Co. v. Redington, 442 U.S. 560, 99 S.Ct. 2479, 61 L.Ed.2d 82 (1979).

<sup>103</sup> See Middlesex County Sewerage Authority v. National Sea Clammers Ass'n, 453 U.S. 1, 101 S.Ct. 2615, 69 L.Ed.2d 435 (1981); Northwest Airlines, Inc. v. Transport Workers Union of America, 451 U.S. 77, 101 S.Ct. 1571, 67 L.Ed.2d 750 (1981); Texas Industries, Inc. v. Radcliff Materials, Inc., 451 U.S. 630, 101 S.Ct. 2061, 68 L.Ed.2d 500 (1981); California v. Sierra Club, 451 U.S. 287, 101 S.Ct. 1775, 68 L.Ed.2d 101 (1981).

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.<sup>104</sup> 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, 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 clarifying the standard which applies to a previously existing duty.<sup>105</sup> 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.<sup>106</sup> 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 preempted a field of the law, they have still

---

<sup>104</sup> See, Morris, *The Role of Criminal Statutes in Negligence Actions*, 49 COLUM. L.REV. 21, 34 (1949).

<sup>105</sup> See, 3 Harper, et al., *The Law of Torts* § 18.6 (2d ed.1986); Keeton, et al., *Prosser & Keeton on the Law of Torts* § 56, at 373-77 (5th ed.1984).

<sup>106</sup> See Keeton, et al. § 36, at 221 n. 9; Forell, *The Statutory Duty Action in Tort: A*

concluded that the traditional state and territorial law remedies continue to exist for violation of those standards.<sup>107</sup> Because a courts declines to imply a federal right of action the federal statutes may create a standard of conduct which, if broken, would give rise to an action for common-law negligence.<sup>108</sup> 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.<sup>109</sup> Given the express intention of Congress and the drafters of the Rules not to preempt any state laws granting greater rights to privacy in personal health information<sup>110</sup> 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.

---

*Statutory/Common Law Hybrid*, 23 Ind. L. Rev. 781, 782 (1990).

<sup>107</sup> See, e.g., Abdullah v. American Airlines, Inc., 181 F.3d 363, at 375 (3<sup>rd</sup> rd Cir. 1999).

<sup>108</sup> Iconco v. Jensen Construction Co., 622 F.2d 1291, 1296 (8th Cir.1980); Hofbauer v. Northwestern Nat. Bank of Rochester, Minn., 700 F.2d 1197, at 1201 (8<sup>th</sup> Cir. 1983).

<sup>109</sup> Id. citing Iconco v. Jensen Construction Co. at 1298.

<sup>110</sup> Cite to Statute.

Since a violation of the HIPAA Privacy Rules by a healthcare provider which 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.

*Liability for Disclosure to Employers*

The advent of the Employee Retirement Income Security Act of 1976 (ERISA), 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. 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. As plan administrator, an employer is able to review all claims paid by the administration company which necessarily 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 which 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.<sup>111</sup>

---

<sup>111</sup> ERISA, sec. 502(a), codified at 29 U.S.C. sec. 1132. See Mary Anne Bobinski,

---

*Unhealthy Federalism*, U.C. Davis Law Review 24, 255 (1990). *See also*, Mark A. Rothstein, *Genetic Discrimination in Employment and the Americans with Disabilities Act*, Houston Law Review 29, 980-981 (1992).

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 be healthcare providers or insurance companies, have developed a culture in which there is a relatively high degree of respect for the confidentiality of medical records. Although some large employers such as IBM have instituted internal controls on access to employee health information, many employers maintaining self-funded health plans do not have this same culture of respect for confidentiality.

While many if not most companies in the healthcare industry have begun to focus seriously on the problem of conforming their internal privacy and confidentiality practices to conform with the Health Privacy Rules, it does not appear that a similar compliance effort has begun by large employers maintaining health plans. Not all employers may be aware that their previous practice of accessing personal health information from health plans maintained by employers and using that information for purposes of making employment decisions will now be prohibited. 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 an employer only if one of four requirements are 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;
- 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.<sup>112</sup>

Thus, except for these limited instances, the Rules would appear to end the practice of employers surreptitiously accessing personal health information and using it in making employment decisions. Doctors, hospitals and health care 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.

---

<sup>112</sup> 45 C.F.R. § 164.512(b)(1)(ii).

Even more significant than the potential criminal and administrative enforcement proceedings against such employers is significantly increased liability under state common law breach of confidentiality theories. Such theories are very likely to be pursued in the context of employment disputes when it appears that employers have accessed employee medical information outside of the context of the Rules. The success of such actions is likely to be determined by the question whether employers can have duties of confidentiality under state common law. As we have seen, there has been a developing trend in the common law finding employers liable under an “inducement to breach of confidentiality,” illustrated by such as Alberts v. Devine,<sup>113</sup> and Morris v. Consolidation Coal Co.<sup>114</sup> However, in such cases, the employers did not have a pre-existing duty, but the duty was derivative of that of the physician. By defining an employer who sponsors a self-funded health plan as a “covered entity,” the HIPAA Privacy Rules place a duty of confidentiality directly on the employer. It thus remains to be seen whether employers will become as common as doctors and other health care providers as defendants in breach of confidentiality actions.

### **Downstream Liability for Business Associates**

As we have seen, the Rules lack any sanctions which apply to Business Associates of Covered Entities, and since many improper disclosures of personal health information may be the responsibility of such Business Associates, the lack of express administrative or criminal sanctions for improper disclosure by these entities has been considered a defect in the Rules. The Rules as they were originally proposed required all contracts between Covered Entities and

---

<sup>113</sup> 395 Mass. 59, 479 N.E.2d 113 Mass. (1985).

<sup>114</sup> 191 W.Va. 426, 446 S.E.2d 648 W.Va. (1994).

Business Associates to designate patients as the “third party beneficiaries” of the contracts, but this provision was removed from the Rule in its final form in the face of considerable controversy.

As we have seen in the discussion of “downstream” liability for inducement to breach of confidentiality under the common law, the problem of applying a duty of confidentiality to downstream users of medical information is the most critical question presented in today’s world of confidentiality. This is particularly critical given the fact that most downstream users of medical information access electronic medical information. While not expressly creating liability on the part of such Business Associates, the requirement in the Rules that all secondary disclosures to Business Associates take place pursuant to a “business associate contract,” puts the downstream users or Business Associates on notice that they also have a duty of confidentiality to patients which is similar to the duty owed patients by a doctor. Under the common law “inducement” to breach of confidentiality tort, it is critical to establish the third party had notice that the information was obtained through a confidential relationship and a duty to treat the information confidentially. The Rules provide the critical element of this tort, *notice*.

Under the Rules, all downstream users of medical information under contracts with the Covered Entities should be on notice of their duty to maintain the confidentiality of the information and potentially liable under the common law for breach of that duty. The Rules do not create a private cause of action, but given that a private cause of action already existed in the common law, what was missing to establish clear downstream liability was the factual predicate of notice and a duty. Given these predicates, the common law may well find that patients are “third party beneficiaries” of business associate contracts even after such provisions were

eliminated from the final Rules. Alternatively, the patients may be found to have claims under the inducement to breach of confidentiality theories when wrongful disclosures take place by secondary users of personal health information.

Another theory which may be viable in this context is an agency theory. The requirement of the Rules that there be a contract between Covered Entities and their business can be argued to make Business Associates 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 for the violation of a duty owed by the principal. The covered entity, as the principal, may well have a defense of the exercise of reasonable care which can be shown by a contract requiring the business association to protect personal health information according to the standards of the HIPAA Privacy Rules. However, the failure by the Business Associate to conform with these standards should allow a plaintiff to show direct liability under the common law breach of confidentiality theory on the part of the Business Associate.

One problem with establishing third party or downstream liability in the past has not been for lack of instances in which third parties have misused personal health information. Rather, it is the difficulty of discovering such breaches of confidence. Biddle involved an internal whistleblower at the law firm. Other instances have been discovered in the context of personal injury litigation. Most breaches of confidence by Business Associates are not prosecuted because they are not discovered. The requirement of an accounting of secondary disclosures contained in the Rules potentially change the current system in which breaches of confidence by Business Associates often can remain unknown. The requirement that both the covered entity and the Business Associate maintain an accounting of all disclosures to third parties for purposes other

than treatment and payment makes transparent the breaches of confidentiality which previously were opaque.

### **Confidentiality and the First Amendment**

The application of breach of confidentiality theories to protect personal health information raises important questions whether such tort laws may be in tension with the First Amendment. 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.<sup>115</sup> At least two other articles have concluded that the breach of confidentiality tort would be to subject to a strong challenge under the First Amendment.<sup>116</sup> The concerns about the constitutionality of restrictions on the disclosure of personal health information arise from a series of cases in which the Supreme Court has struck down as violating the First Amendment's

---

<sup>115</sup> *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).

<sup>116</sup> Susan M. Giles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 Buff. L. Rev. 1, 62-83 (1995); Michael Frankel, *Do Doctors have a Constitutional Right to Violate Their Patients' Privacy?: Ohio's Physician Disclosure Tort and the First Amendment*, 46 Villanova Law Review 141, 16-169 (2001).

freedom of expression various attempts by the state and federal government—both as a matter of civil or criminal statute as well as a matter of common law--to protect personal privacy.<sup>117</sup>

---

<sup>117</sup> New York Times v. United States, 403 U.S. 713 (1971); Cox Broadcasting v. Cohn, 420 U.S. 469 (1975); Florida Star v. B.J.F., 491 U.S. 524 (1989); Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978); Oklahoma Publishing Co. v. District Court, 430 U.S. 308 (1977); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979) Bartnicki v. Vopper, 532 U.S. 514; 121 S.Ct. 1753 (2001).

One of the clearest expressions of the constitutional infirmity of attempts to regulate information under the rationale of protecting privacy is found in the plurality opinion of Justice Stevens the most recent Supreme Court case on the topic, Bartnicki v. Vopper.<sup>118</sup> 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<sup>119</sup> which created a civil cause of action against any person who, knowing or having reason to know that the communication was obtained through an illegal interception, willfully disclosed its contents. The Court held that to the extent that the statute purported to create liability for a publishing lawfully obtained information from a source who obtained it unlawfully, the statute violated the First Amendment's protection of freedom of speech. In his plurality opinion striking down the statute, Justice Stevens noted that "the naked prohibition against disclosures is fairly characterized as a regulation of pure speech."<sup>120</sup> Stevens went on to note that "[a]s a general matter, 'state action to punish the publication of truthful information seldom can satisfy constitutional standards.'"<sup>121</sup> Stevens went on to note that "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."<sup>122</sup> While the scope of the plurality opinion in Bartnicki was limited to matters of

---

<sup>118</sup> 531 U.S. 990 (2001).

<sup>119</sup> Title 18 U.S.C. § 2511(1)(a).

<sup>120</sup> Bartnicki v. Vopper, 531 U.S. at \_\_\_\_; 121 S.Ct. at 1759.

<sup>121</sup> Id. at 121 S.Ct. 1762 citing Smith v. Daily Mail Publishing Co., 443 U.S. at 102 (1979).

<sup>122</sup> Id., citing Smith v. Daily Mail Publishing Co., 443 U.S. at 102, Florida Star v. B.J.F.,

public concern and did not prohibit laws protecting speech which was merely a matter of private concern, and while a separate concurrence by Justice Breyer joined by Justice O'Connor attempted to leave room for other legal attempts to protect personal privacy by regulating disclosures of information, 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.

---

491 U.S. 524, and Landmark Communications, Inc. v. Virginia, 435 U.S. 829.

It is the thesis of this article that the extent that the HIPAA Privacy Rules create a right limiting the disclosure of their personal health information, irrespective of the existence of a relationship of trust, the protections created by the Rules would appear to be subject to constitutional attack under the First Amendment at least as such protections are applied to private individuals and institutions.<sup>123</sup> 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.

It should be noted 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 an individual right, and where it exists, it gives individuals control, to a greater or lesser degree,

---

<sup>123</sup> The restriction of disclosure of personal information by the government does not raise legal issues under the First Amendment. Statutes such as the Federal Privacy Act governing governmental disclosures of personal information have been held to be generally unproblematic under Constitutional analysis. 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). Also see, United States v. Westinghouse, 638 F.2d 570 (3rd Cir. 1980).

over the use, access and disclosure of their individually identifiable health information, independent of the relationship with a healthcare provider. A general right of privacy may be inherently problematic under the First Amendment. However, if the Rules are understood not as creating a “right of privacy” in personal health information, but as implementing the quite different duty of confidentiality with respect to specific Covered Entities and Business Associates, the Rules can be seen not as attempting to regulate personal health information based on the private nature of that information, but only *regulating the relationships* in which such information is exchanged the constitutional concerns diminish.

In the decisions of the Supreme Court, the clash between the protection of information and the First Amendment interest appears to be sharpest when there is no preexisting relationship between the subject of the information and the person disclosing the information which could give rise to an explicit or implicit expectation of confidentiality. The distinction between the presumptive constitutionality of laws which place duties of non-disclosure when there exists an independent duty or relationship of trust and the presumptive constitutional scrutiny with respect to laws placing duties of non-disclosure on individuals and entities when no such relationship of trust exists was first articulated by the Supreme Court in Landmark Communications, Inc. v. Virginia.<sup>124</sup> The distinction was made express in Cohen v. Cowles Media,<sup>125</sup> when the Supreme Court held that the First Amendment did not prohibit a news source recovering damages from a

---

<sup>124</sup> See also, 435 U.S. 829, 841 and n. 12 (1978) (It can be assumed for purposes of decision that confidentiality of 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.)

<sup>125</sup> 501 U.S. 663 (1991).

newspaper publisher under promissory estoppel law for publishers' breach of promise of confidentiality given in exchange for the information. In general, the clash between the protection of information and the First Amendment interest appears to be sharpest when there is no preexisting relationship between the subject of the information and the person disclosing the information which could give rise to an explicit or implicit expectation of confidentiality.<sup>126</sup>

When the language in the Rules regarding the creation of a “right to privacy” in health information is recognized as largely precatory, one can see that those provisions of the Rules which are actually engaged in the concrete work of protecting personal health information adopt a traditional confidentiality model--not a privacy model of regulation of information. The Rules do not apply until there exists a previously existing professional or contractual relationship between patient and healthcare provider. As such, the Rules do not create a general right to control the disclosure of personal health information. The Rules do not regulate information, they regulate relationships.

The Rules generally codify at a federal level the same standards of confidentiality based on relationships of trust established by the common law. Both the common law tradition of confidentiality 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

---

<sup>126</sup> See generally, 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).

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 as a codification of traditional common law confidentiality doctrines. Even in the most novel portion of the Rules, their implementation of fair information practices, use 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, regulation of the use and disclosure of personal health information within the context of a contractual or professional relationship of confidentiality appear 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; between healthcare providers and plans; and between 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.

In the context of a such a system of relationships between a patient and a healthcare provider, of a patient and an 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 who obtains personal health 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<sup>127</sup>. It should be cautioned, however, in the context of contracts required by law, particularly as applied to downstream entities without a relationship with a patient, as the duty of confidentiality becomes more attenuated. The farther away from the patient, and the more abstract the contractual structure, the more likely it becomes that attempts to find Business Associates liable for breach of confidentiality will be found to violate First Amendment principles. In general, however, within the culture of the health care industry, it is well understood that Business Associates who misuse personal health information do so in violation of their contractual duties to Covered Entities as well as with the patients. As such, the application of breach of confidentiality theories as to such entities does not raise the same

---

<sup>127</sup> See e.g., Snepp v. U.S., 444 U.S. 507 (1980) (upholding a lower court injunction of the publication of a book by a CIA officer who had contractually agreed to permit CIA pre-publication review of his materials).

constitutional concerns as many other attempts to protect information under the rationale of a “right to privacy.”

### **Costs and Benefits**

It is the thesis of this article that Rules do not represent a dramatic alteration in the rules governing healthcare providers. As such the extremely high cost estimates associated with their implementation are a matter of considerable interest.<sup>128</sup> Representatives of Hospitals and Medical Schools have asserted in testimony to Congress that compliance with the Rules is likely to result in greater inefficiencies and higher costs, not to mention the potential detrimental impact on vital healthcare research.<sup>129</sup> It appears that generally the HIPAA Privacy Rules did not significantly change the standards of confidentiality already applicable to healthcare providers. 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 28 states already provided a right for patients to review their medical records and to recommend changes or amendments if necessary.<sup>130</sup> Various federal health benefit programs such as the Medicare program also imposed similar requirements.<sup>131</sup>

---

<sup>128</sup> The cost estimates are quite high, ranging from an estimate by the Office of Management and Budget of \$17.6 billion over ten years for the entire healthcare industry to a much higher estimate by the American Hospital Association of \$22 billion just for hospitals. A study conducted by the Blue Cross/Blue Shield Association estimated that individual hospitals will incur costs of between \$775,000 and \$6 million to pay for some aspects of complying with the rules.

<sup>129</sup> Dr. G. Richard Smith, on behalf of the Association of American Medical Colleges, February 8, 2001, testimony presented to Senate Committee on Health, Education, Labor and Pensions. (Research impacted negatively). John Houston, on behalf of the American Hospital Association. (Rule fails to find right balance between individual privacy and societal good).

<sup>130</sup> For the Record: Protecting Electronic Health Information, p. 40, National Research

---

Council, 1997.

<sup>131</sup> See, e.g., the Privacy Act, Public Law 93-579, 5 U.S.C. Sec. 552a; Medicare Conditions of Participation for Hospitals, Sec. 482.24; Regulations governing privacy of drug and alcohol abuse treatment programs, 42 U.S.C. §§ 290dd-3 and 290ee-3 (1988). Previous federal regulations provided protection for HIV status and drug and alcohol abuse medical records. Also, privacy protections existed for the medical records of beneficiaries of federal healthcare programs, such as Medicare and Medicaid, as well as generally under the Federal Privacy Act.

One explanation of the increase in costs associated with the 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.<sup>132</sup> Traditional standards for confidentiality which 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.<sup>133</sup> The problem of the management of electronic information is not unique to healthcare and challenges numerous other businesses which create, manage and store large amounts of sensitive personal information.<sup>134</sup> 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 which are obtained from the growth in the use of electronic health information also bring with them potential dangers.

---

<sup>132</sup> Interestingly, the cost estimates prepared by the Office of Management and Budget, appear to place a relatively low cost for providers purchasing of new computer hardware and software systems, and higher costs for the cost of personnel, issuing new forms and training.

<sup>133</sup> Ronald J. Mann & Jane K. Winn, Electronic Commerce, ch. 1, forthcoming (2002).

<sup>134</sup> See, e.g., Gramm, Leach, Bliley bill.

It is the thesis of this article that the task of balancing the benefits of electronic health information against the risks to 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. If this is correct, the fact that the high cost estimates of an industry's compliance with the Rules may be self inflicted does not resolve the question is what the cost and the benefits are of such a possible expansion of private causes of action under breach of confidentiality theories. 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 may be 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 which affects the patient's life. Even if the person close to the patient operates with the best of intentions, their obtaining sensitive medical information may be more threatening than unauthorized access to medical records by a stranger with nothing but prurient motivations. 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 a community, family, friends, neighbors, customers and clients. This lower level of danger with respect to disclosure of health information to strangers contrasts

sharply with the dangers associated with disclosure of information typically considered “private.” Within the context of privacy, a “peeping tom” is just as offensive if he is a stranger as it is if he is a neighbor or family member, if not more so.

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 its lack of relevance, 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 in which the chain of trust has been broken.

A system of legal rules should ideally encourage the holder of information to weigh the risk of harmful disclosure against the resources which 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 is limited in the absence of damages. The common law operates under a “no harm, no foul” approach. Unauthorized access, even by strangers which 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, typically results in an award of nominal damages.

The reviewing of individually identifiable medical information about an individual by a stranger with no ulterior purpose other than the processing of the claim, the review of drug interactions, the identification of lower cost alternatives, or the education of the provider or patient does not present any serious likelihood of damages to the subject of that information. The ability of cleaning staff to access confidential patient records, even the inadvertent disclosure to hospital cleaning staff which does not result in harm to the patient, should not cause the expenditure of massive social resources to protect against such events. The common law standard of care permits the health information manager to exercise some discretion in determining to whom access is to be allowed in the course of treatment. As such 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.

### **Conclusion**

In summary, both the common law and the HIPAA Privacy Rules adopt a model based on the tort law concept of the balancing of costs and benefits. It is the thesis of this article that 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.