

## The National Health Information Network and the Future of Medical Information Privacy

**Edward J. Szewczak**

Information Systems Department  
Canisius College  
Buffalo, NY 14221  
[szewczak@canisius.edu](mailto:szewczak@canisius.edu)

### ABSTRACT

*Medical information has a special status among the various items of personal information. The introduction of information technology (IT) has changed the handling of medical information in ways that are both promising for improving health care as well as threatening to the individual patient's medical information privacy.*

*The challenge to business practitioners is to manage medical information intelligently and to avoid the negative consequences of mismanaging this information, which may include customer backlash in the forms of boycotts, lawsuits, and loss of company reputation. This challenge is particularly important in the context of the U.S. National Health Information Network initiative, which has the potential of sending electronic medical information to IT devices worldwide in the not too distant future.*

### INTRODUCTION

In his 2004 State of the Union address, President George W. Bush stated that, by computerizing health records, it would be possible to avoid dangerous medical mistakes, reduce medical costs, and improve medical care ([www.whitehouse.gov/news/releases/2004/01/20040120-7.html](http://www.whitehouse.gov/news/releases/2004/01/20040120-7.html) accessed June 3, 2006 from the White House website). Drawing on a report from the Institute of Medicine (2001) and on the conclusions of a panel of IT experts, Kaushal *et al.* (2005) reported that the creation of a National Health Information Network (NHIN) electronically connecting together physician's offices, hospitals, skilled nursing facilities, home health agencies, clinical laboratories, payers, and pharmacies will be possible at a cost of \$156 billion.

Though the NHIN will undoubtedly result in money savings and an increase in the quality of medical care, it will also have major implications for the future of medical information privacy. This paper will examine these implications from the perspective of the business organization. Since all business organizations will have access to individuals' medical information in the near future, managers must be aware of the importance of handling medical information properly so as to avoid potential damage to his/her organization.

### ***Medical Information Privacy***

An individual's medical information can take many forms such as text, photographs, video, x-ray, sound, etc. One definition of information that is directly relevant to medical information privacy is *data that have been evaluated to be relevant and useful for making particular decisions or classes of decisions* (King and Epstein, 1976). Though the account was originally provided for the context of business management decision making, it is clearly applicable to the situation of various medical practitioners. Data on patients are collected and stored with a view toward retrieving them later to aid physicians and other health professionals in making informed, intelligent decisions that will lead to better patient health. Evaluation is central in this setting since it is the medical practitioner who judges whether or not the data are relevant and useful in a specific context. Data that are relevant and useful in a specific context take on the status of information. Data that are not relevant and useful in a specific context remain simply data that may become relevant and useful at another time and/or in another context by a medical practitioner or someone related to or allied with a medical practitioner either directly or indirectly (e.g. a business associate).

Cate (1997) identified a number of conceptions of what constitutes privacy from the literature. Privacy has been viewed as an expression of one's personality or personhood, focusing on the right of the individual to define his or her essence as a human being; as autonomy – the moral freedom of the individual to engage in his or her own thoughts, actions, and decisions; as citizens' ability to regulate information about themselves, and thus control their relationships with other human beings; and as secrecy, anonymity and solitude. In the area of medical information, the definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7) is appropriate.

The Westin definition is consistent with the confidential relationship between doctor and patient. Confidentiality refers to how data collected for approved purposes will be maintained and used by the individual, group or institution that collected it, what further uses will be made of them, and when individuals will be required to consent to such uses. In this regard, privacy may be construed as a balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing the information for the purposes of medical research and public health management, and how the balance is codified into legislation giving individuals the means to control information about themselves (Office of Technology Assessment, 1993; Rindfleisch, 1997).

### ***The Medical Record***

Traditionally medical data were collected and stored as records in physician's offices and in hospitals. Often the data were recorded manually and retrieved manually. Patient data forms the *medical record* and its contents ([www.eff.org/Privacy/Medical/1993\\_ota\\_medical\\_privacy.report](http://www.eff.org/Privacy/Medical/1993_ota_medical_privacy.report); retrieved June 8, 2006 from the Electronic Frontier Foundation website). Medical records may contain patient

data such as name, address, age, next of kin, names of parents, date and place of birth, marital status, religion, history of military service, Social Security number, name of insurer, complaints and diagnoses, medical history, family history, previous and current treatments, an inventory of the condition of each body system, medications taken now and in the past, use of alcohol and tobacco, diagnostic tests administered, and findings, reactions and incidents. Records may also contain subjective information based on impressions and assessments by health care workers such as mental ability and psychological stability and status. In addition to data about the patient's current condition, a patient's medical record may also contain the results of genetic research and testing that enable predictions of future medical conditions and the prospects of developing specific medical problems.

Typically the creation and maintenance of medical records was done by manually health professionals. But IT has changed this practice (Kilman and Forslund, 1997). Notes hand-written by doctors and nurses are being put into electronic form in the name of faster, more extensive access to needed information. Healthcare companies are competing to get doctors to write prescriptions over the Internet and to persuade people to place their personal health records on the Internet (Consumer Reports, 2000). Companies have made available software that an individual can use to create an Internet-based "personal health record" that can be used to organize family medical histories, including medical conditions, medications and allergies. These personal records may be transmitted to health professionals over a computer network (Rubenstein, 2005).

Medical records are available online to medical practitioners for the purposes of decision making and improving healthcare. They are also available to other users and institutions in non-treatment contexts. Medical records are used to conduct federal government-mandated medical community audits of physician competency and performance. They are also used by insurance companies in the assessment of an applicant's eligibility for health and life insurance and in claims processing to detect medical fraud. Medical information is also used by private employers, educational institutions, credit investigators, and law enforcement agencies for a variety of non-medical reasons.

### **PERSONAL AND SOCIAL CONCERNS ABOUT MEDICAL INFORMATION PRIVACY**

As personal information, medical information has a special status. As Krzysztof and Moore (2002) observe (p. 15):

Medical information about the individual patient is considered highly private, and the general public is extremely fearful about disclosure....We all enjoy the benefits of medical research conducted on other patients, but we are very often reluctant to contribute or release our own information for such purposes. When medical data are published it is expected that the researchers will maintain the dignity of the individual patient, and that the results will be used for socially beneficial purposes.

This observation has been supported by various public opinion polls conducted since 1993 that have uncovered a basic concern people have about the privacy of their medical records and how these records may be used ([www.epic.org/privacy/medical/polls.html](http://www.epic.org/privacy/medical/polls.html); retrieved April 17, 2006 from the Electronic Privacy Information Center website). Major areas of concern are:

*Employment/career advancement.* People are concerned that employers may use personal health information to limit job opportunities. They are also concerned that medical information will be used for many non-health purposes, such as determining promotions and job advancement.

*Insurance eligibility.* People are concerned that insurance companies may use personal health information to deny an application for various kinds of insurance coverage (e.g. medical insurance).

*Computerized versus paper records.* The trend toward computerizing the healthcare system and keeping records electronically threatens medical information privacy. People feel more secure when medical records are kept in paper form.

*Genetics research.* People do not want medical researchers to be allowed to study an individual's genetic information without obtaining the individual's consent.

*Medical records security.* People feel protecting the confidentiality of medical records is essential to health care reform. Weak data security may lead to leaks of sensitive health information. People also think that insurance companies get more information from doctors than is needed.

*Mistrust of government.* People worry that existing federal health privacy rules protecting patient information may be reduced or ignored in the name of efficiency. In addition, people fear that government agencies and researchers are allowed to see medical records without a patient's permission.

It should be noted that much of the business research that has been done on information privacy has focused on individual consumers' *general* attitudes and concerns about their information privacy (Straub and Collins, 1990; Culnan, 1993; Dhillon and Moores, 2001) and the development of instruments to gather data about these attitudes and concerns (Smith, Milberg and Burke, 1996; Malhotra, Kim and Agarwal, 2004). The fact that people care about their privacy is generally evident from instances of public outcry in reaction to companies' seeming insensitivity to privacy concerns. For example, in 1990 Equifax and Lotus Development Corporation produced a series of computer disks on which were stored the names, addresses, buying habits and income information of roughly 120,000,000 American consumers. The disks were made available for sale to the public. Consumer inquiries and complaints caused the companies to discontinue the disks (Culnan, 1993). In another more recent example, Facebook.com added a feature that makes it easier for users to keep abreast of their friends by tracking users' activities on the website. It then communicated these activities to all the people in the friends'

social network. In an apparently unexpected reaction, hundreds of thousands of Facebook.com users expressed outrage at what they perceived as an unwarranted use of their personal information (Warren and Vara, 2006). On the basis of these incidents, it appears highly likely that people's response to the mishandling of their medical information will result in a negative reaction against any organization responsible for the mismanagement of this special class of information.

## THE ROLE OF LEGISLATION

One might think that legislation addressing the issues and problems of safeguarding medical information would solve many of the problems involving the mishandling of medical information. However, the effectiveness of legislation in establishing and maintaining medical information privacy is questionable at best, despite legislative efforts to the contrary. The U.S. Bill of Rights does not address privacy issues at all. However, in *Griswold v. Connecticut* (381 U.S. 479 (1965)), the Supreme Court found sources for a right to privacy in the First, Third, Fourth, Fifth and Ninth Amendments to the Constitution in the form of "zones" or "penumbras" of privacy ([www.eff.org/Privacy/Medical/1993\\_ota\\_medical\\_privacy.report](http://www.eff.org/Privacy/Medical/1993_ota_medical_privacy.report); retrieved May 22, 2006 from the Electronic Frontier Foundation website). A major modern discussion of an information privacy right is *Whalen v. Roe* (429 U.S. 589 (1977)) wherein the Supreme Court accepted that a right of privacy includes a generalized "right to be let alone," which includes "the individual interest in avoiding disclosure of personal matters." The Court noted that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." However, the Court has not expanded on this idea in any significant way (National Research Council, 1977).

Federal and state governments have attempted to deal with privacy issues in ways that satisfy the needs of various stakeholders such as doctors, insurance companies, researchers, law enforcement, and data processing firms as well as individuals. The result has been various legislative measures that provide legal compromise. For our purposes, the most significant measure is the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

### ***The Health Insurance Portability and Accountability Act of 1996***

The first comprehensive set of federal regulations of health information is provided by HIPAA. It provides for two rules related directly to medical information privacy: the Privacy Rule (45 Code of Federal Regulations 164.500 – 164.534) and the Security Rule (45 Code of Federal Regulations 164.103 – 164.318) ([www.archives.gov/federal-register/index.html](http://www.archives.gov/federal-register/index.html); retrieved June 10, 2006 from the Federal Register archives website).

### ***The HIPAA Privacy Rule***

The HIPAA Privacy Rule provides the federal floor of privacy of protected health information (PHI) in the U.S. It only applies to medical records maintained by "covered

entities” (health care providers, health plans, and health care clearinghouses/data processing firms) in any form (electronic or non-electronic, including oral). It allows more stringent state laws to continue in force. An individual has a number of rights under the Privacy Rule including the following (adapted and expanded from [www.epic.org/privacy/medical](http://www.epic.org/privacy/medical); retrieved April 17, 2006 from the Electronic Privacy Information Center website):

- To access, inspect and copy PHI held by hospitals, clinics, health plans and other “covered entities” with some exceptions
- To request amendments to PHI held by covered entities
- To request an accounting of disclosures that have been made without authorization to anyone other than the individual for purposes other than treatment, payment and “health care operations” (i.e., medical practice evaluations for accreditation conducted by organizations such as the Joint Commission for the Accreditation of Healthcare Organizations and the National Committee for Quality Assurance)
- To receive a Notice of Privacy Practices from doctors, hospitals, health plans and others in the healthcare system
- To request restrictions on uses and disclosures of PHI
- To complain about privacy practices to a covered entity and to the Secretary of Health and Human Services

Security risks to medical information may come from inside a business as well as from external sources. There are a number of internal security risks such as accidental disclosures, insider curiosity, releasing medical information to outsiders for revenge, spite or profit, and uncontrolled support functions (Rindfleisch, 1997). The Privacy Rule includes civil and criminal penalties for violations of an individual’s privacy. Criminal penalties can approach \$250,000 and/or 10 years imprisonment if the offense is committed with intent to sell, transfer or use PHI for commercial or personal gain, or for malicious harm. The Office of Civil Rights (OCR) is charged with enforcing the Privacy Rule.

The HIPAA Privacy Rule does *not* prohibit the disclosure of PHI when such disclosure is required or permitted by other federal law. For example, the Gramm-Leach-Bliley Act does not prohibit the sharing of information among affiliated companies (such as banks and brokerages, which are *not* covered entities). So an individual’s credit card account transactions may include data about where an individual goes for health care, and this data may be shared among affiliated companies and is not protected by HIPAA. The HIPAA Privacy Rule also explicitly includes exceptions to the rules for use and disclosure. In fact, there are a number of uses and disclosures of information for which an authorization or opportunity to agree or object is *not* required (for example, for judicial and administrative proceedings, and for law enforcement purposes), including the use of PHI for marketing purposes (which, according to the Department of Health and Human Services, may be too difficult to distinguish from treatment purposes) ([www.privacyrights.org/fs/fs8a-hipaa.htm](http://www.privacyrights.org/fs/fs8a-hipaa.htm); retrieved June 16, 2006 from the Privacy Rights website).

It should be noted that there may be different incentives at work on the parts of health care providers and data collection organizations. The health care provider may wish to secure services in the patient's best interest without disclosing unnecessary information. The data collection organization may be motivated mainly by financial considerations (Yang & Kombarakaran, 2006). The HIPAA Privacy Rule is particularly difficult to implement when it comes to managing business associates under contract who perform an action on the health care provider's behalf and to whom the health care provider is releasing PHI. These business associates often have free access to a patient's PHI. They include people such as insurance agents, billing agents, consultants, and transcriptionists. If a health care provider discovers that a business associate has breached or violated a contract with respect to safeguarding PHI, the health care provider must take reasonable steps to remedy the problem or terminate the contract. If the contract cannot be terminated, the health care provider must report the problem to the OCR, which may exact civil penalties against the business associate (Wilson, 2006).

However a health professional may not know that a business associate has breached or violated a contract with regard to safeguarding PHI. Because HIPAA does not prohibit the sharing of PHI among various covered entities or their business associates, PHI could be used in ways other than for treatment or billing. For example, an individual could be charged higher loan rates because of some piece of data in his/her medical record, and it would be impossible to prove the data were shared because there is no required disclosure audit for non-covered entities.

In addition, data networks may be Internet-based and global in reach. Individual health records may be transmitted overseas and handled by subcontractors in ways the individual is completely unaware of and would object to under any circumstances. Another related security challenge is the data breach. A hacker or even a trusted employee can steal data from a computer system and offer them for sale to interested parties (Consumer Reports, 2006). Also, if the history of dotcom business is any guide, companies that run into financial difficulties may choose to sell customer data to meet obligations, even though the companies have published privacy policies.

### ***The HIPAA Security Rule***

The HIPAA Security Rule provides security standards and implementation specifications for three kinds of safeguards (administrative, physical and technical) to protect PHI in *electronic* form. It also divides the implementation specifications into required and addressable (i.e., not required but recommended). Covered entities have a certain amount of flexibility in implementing addressable specifications. In deciding which security measures to adopt, the covered entity must consider its own size, complexity and capabilities, its technical infrastructure, hardware and software security capabilities, the costs of the security measures, and the probability and criticality of potential risks to electronic PHI. For example, covered entities may choose to adopt encryption as a technical safeguard for the transmission security standard. But since encryption is given as an addressable implementation specification, it is not required by HIPAA but simply

recommended. In addition, while encryption and other technologies may keep patient data private and secure, it is what people who have access to the decrypted data do with it that is important to the issue of medical information privacy (Rindfleisch, 1997; Patton, 2005).

HIPAA is not specific as to the exact technology that should be used to implement transmission security, since technology changes and progresses in ways that are difficult to predict. Current implementation of transmission security will most likely involve the use of firewalls, user authentication, encryption/decryption, anti-virus/malware software, and anonymizers (Cheng & Hung, 2006). These implementation choices will be replaced as newer, more effective technologies become available.

## **THE NATIONAL HEALTH INFORMATION NETWORK**

The U.S. federal government is promoting a national system of electronic health records (EHRs) and the building of a National (aka Nationwide) Health Information Network (NHIN) which will connect EHRs to health care providers, insurers, pharmacies, laboratories, and claims processors (Kaushal, et al., 2005). HIPAA makes explicit mention of Electronic Data Interchange (EDI). However implementation of EDI by covered entities has resulted in many proprietary EDI formats, resulting in a lack of common industry-wide standards. This lack of uniformity is viewed as a major obstacle to realizing potential efficiency and savings (45 Code of Federal Regulations Part 162). Since EDI has been replaced by the use of TCP/IP in Internet networks, it is likely that any future NHIN will use TCP/IP as its fundamental protocol, perhaps together with legacy systems for a time ([www.amia.org/pubs/symposia/D005234.pdf](http://www.amia.org/pubs/symposia/D005234.pdf); Retrieved September 3, 2006 from the American Medical Informatics Association website); Deshmukh & Croasdell, 2005; Cheng & Hung, 2006). Four companies (Accenture, Computer Science Corporation, IBM and Northrop Grumman) have been selected the Department of Health and Human Services to develop regional versions of the NHIN with a view toward developing interoperability in the near future.

### ***Medical Databases***

Medical databases will be major sources of medical information on the NHIN. However a database is implemented, the EHRs comprising it will be accessed by many interested parties over the NHIN.

One of the largest central databases of EHRs is the Medical Information Bureau (MIB). It is shared by insurance companies to obtain information about life insurance and individual health insurance policy applicants. If the applicant reports a condition that the insurer considers significant, or if the results of a required examination, blood test, or urine test raise questions for the insurer, the insurer will report that information to the MIB. MIB EHRs consist of codes indicating a particular condition or lifestyle (such as the individual smokes cigarettes). As such, MIB does not include the totality of an individual's medical record ([www.privacyrights.org/fs/fs8a-hipaa.htm](http://www.privacyrights.org/fs/fs8a-hipaa.htm); retrieved June 16, 2006 from the Privacy Rights Clearinghouse website)

Another example is the Children's Hospital of Philadelphia (CHOP). CHOP is collecting DNA profiles on as many as 100,000 child patients in order to develop an anonymous database that researchers can use to study children's genetic profiles. Research results may reveal which genes underlie problems affecting children such as diabetes, obesity, asthma and cancer. This research could lead to the development of diagnostic tests and drugs. By linking genetic information to EHRs, CHOP may obtain research funds and patents and forge partnerships with drug companies (Regalado, 2006).

There are a number of benefits as well as disadvantages of medical databases ([www.lbl.gov/Education/ELSI/privacy-main.html](http://www.lbl.gov/Education/ELSI/privacy-main.html); retrieved April 26, 2006 from the U.S. Department of Education website). Among the benefits are:

- A patient's medical information would be immediately available to an attending doctor, including life saving information
- Researchers would be able to track certain diseases as well as patients' responses to certain drugs
- Medical databases would allow for better organization and more legibility of medical files
- EHRs may be more secure than paper records since security systems can monitor medical databases

Among the disadvantages of medical databases are:

- Employers may access medical information about their employees which they might use to deny employment or job advancement
- Insurers may use medical information to deny insurance to people they consider to be high risk
- Digitizing medical records will allow many more people legitimate access to medical records, with the increased possibility that the information may be misused by one or more of them

It is important to note that, in general, inaccuracies in databases are widespread and that the ability of individuals to detect these inaccuracies is limited (Straub & Collins, 1990). In addition, the problem of missing values – values accidentally not entered or purposely not obtained for technical, economic or ethical reasons – is widely encountered in medical databases since medical data are collected as a byproduct of patient care activities rather than rigorously collected and evaluated for use in research (Krzysztof & Moore, 2002). These inaccuracies and omissions only accentuate the disadvantages of medical databases.

In addition to medical databases available on the NHIN, there are other sources of medical information available to businesses at large, including company and government databases, public records, and customer volunteered medical information.

### ***Medical Information in Company and Government Databases***

Businesses may acquire medical information that is contained in companies' non-medical databases as a result of acquiring these databases in the course of merger/acquisition activities. They may also have access to medical information in other companies' non-medical databases in the course of maintaining friendly strategic alliances with these companies.

In addition, business associates of healthcare practitioners are in a position to collect and store medical information in company databases for use in business decisions (for example, determining loan rates). As was discussed earlier, HIPAA does not prohibit the sharing of PHI among various covered entities or their business associates.

Various federal, state and local governments maintain databases of personal (including medical) information. As Consumer Reports (2000, p. 23) notes:

The federal government maintains electronic files of hundreds of millions of Medicare claims. And every state aggregates medical data on its inhabitants, including registries of births, deaths, immunizations, and communicable diseases. But most states go much further. Thirty-seven mandate collection of electronic records of every hospital discharge. Thirty-nine maintain registries of every newly diagnosed case of cancer. Most of these databases are available *to any member of the public* [emphasis added] who asks for them and can operate the database software required to read and manipulate them.

Although many of these government database records are stripped of information which could be used to identify individuals (such as Social Security numbers), it is still possible to link the records to private sector medical records using standard codes for diagnoses and procedures employed by the United States healthcare system. The codes are usually included on insurance claims and hospital discharge records. In addition, a patient's anonymity may be compromised by the fact that personally identifiable health information is needed for a variety of research purposes (e.g. to check for duplicate records or redundant cases, and for longitudinal studies) ([www.epic.org/privacy/medical/GAO-medical-privacy-399.pdf](http://www.epic.org/privacy/medical/GAO-medical-privacy-399.pdf); retrieved May 17, 2006 from the Electronic Privacy Information Center website).

Straub & Collins (1990) relate how a user can retrieve information about a specific person from large statistical databases with a small number of unsophisticated queries. As a case in point, a computer privacy researcher at Carnegie Mellon University was able to retrieve the health records of the governor of Massachusetts from an "anonymous" database of state employee health insurance claims by knowing his birth date and ZIP code. The researcher demonstrated that she could do the same for 69% of the 54,805 registered voters on the Cambridge, MA voting list (Consumer Reports, 2000).

### ***Medical Information From Public Records***

Electronically available public records (e.g. court records) are also a source of an individual's medical information (Ogles, 2004). An individual's medical record may be entered into court documents (say, if an individual sues over payment claims) which are available on-line. Public records also have a connection to junk mail, since counties have sold information from public records to commercial companies that then repackage it and resell it to other companies and individuals (Leach, 2004). Junk mail in itself may not be overly troublesome to an individual. But what these companies and individuals may do with public record information in addition to creating and sending junk mail is cause for some concern.

### ***Consumer Volunteered Medical Information***

Much personal health information that is available to the public is volunteered by individuals themselves, by responding to 800 numbers, coupon offers, rebate offers and Web site registration. The information is included in commercial databases like Behavior-Bank sponsored by Experian, one of the world's largest direct-mail database companies. This information is sold to clients interested in categories of health problems, such as bladder control or high cholesterol. Drug companies are also interested in the commercial databases (Consumer Reports, 2000). With the implementation of the NHIN, this interest will be heightened as hospitals link up electronically with doctor offices' records (Landro, 2006).

Data mining is often the rationale for wanting access to medical information. Data mining of medical data offers the health care industry the ability to address issues related to fraud detection and abuse, to profitability analysis, to patient profiling, and to patient retention management (Payton, 2003). However, patients are often unaware that their medical information is being used for data mining purposes, making it unlikely that patients will object to the practice. The challenge to organizations that conduct data mining with medical information is how to respond when and if patients become aware of the data mining. For some patients, the awareness will make no difference; for others, the reaction may be very negative. (See Culnan (1993) for a discussion of what differentiates consumers who object to certain uses of personal information from those who do not object.)

## **MANAGEMENT CHALLENGES OF MEDICAL INFORMATION**

Since companies have relatively easy access to individuals' medical information, the adequate protection of the privacy of this information must be considered an important management challenge, especially in the context of the NHIN.

For healthcare-related businesses, the requirement to safeguard patients' medical information is specified by HIPAA. This includes the following activities (Saul, 2000): adequately safeguard an individual's medical information acquired in

mergers/acquisitions, from public records, from customer volunteers, or simply in the course of doing business (for example, hiring new employees).

- Develop policies to evaluate and certify that appropriate security measures are in place in the business
- Create legal contracts between the business and any business associates given access to individually identifiable medical information requiring the business associates to safeguard the data
- Develop contingency plans for response to emergencies, in a data backup plan and a disaster recovery plan
- Establish a system of access control that includes policies for the authorization, establishment and modification of access privileges
- Perform ongoing internal review of data access records in order to uncover possible security violations
- Supervise systems personnel responsible for systems maintenance activities
- Train system users in system security, including user education on virus protection, monitoring login failures, password management, and how to report discrepancies or suspicious activities
- Establish termination procedures for when an employee leaves the business (voluntarily or involuntarily) or whose data access privileges are revoked

For businesses in industries other than healthcare, the challenges center on how to. Though it is not required by law, businesses should attempt to respect as much as is relevant and possible the rights of individuals under the HIPAA Privacy Rule. For example, businesses should honor individual requests to restrict the use and disclosure of medical information. It is not simply a matter of behaving ethically. Calculating the impact of a potential loss of medical information from a security breach is very difficult. Customer backlash in response to a business' failure to safeguard medical information is a very real and potentially costly possibility. Customer backlash could take the form of a grassroots protest similar to what occurred recently with Facebook.com. Another possibility is an expensive class action lawsuit that could last a protracted period of time. Given how strongly people feel about the privacy of their medical information, either form of backlash could also damage the business' public reputation, especially if the backlash attracts the attention of the various news reporting agencies.

Finally businesses should also conform to the recommendations proposed by the HIPAA Security Rule, especially with regard to transmission security of an individual's medical information. Huston (2001) observes that managers and end users tend not to include security requirements in a system during its design unless they have had the experience of a security breach. Rather than wait for such a potentially damaging event to occur in the sending or receiving of medical information, managers should heed the HIPAA Security Rule recommendations and proactively implement security technology (in particular, encryption/decryption technology) to preempt such an event. In the end, both managers

and their customers will be better served when it comes to the issue of medical information privacy.

## CONCLUSION

Given the potential for mishandling medical information acquired in the course of doing business, management must exercise vigilance in the safeguarding of this information. Though many businesses are not typically interested in acquiring and dealing with medical information, the possible negative consequences of mishandling medical information that is acquired from various sources cannot be ignored. This basic reality will only become magnified once the NHIN becomes a reality, making it technologically possible to inadvertently disseminate medical information nationally as well as internationally. Management must move to preempt these negative consequences before serious damage to the reputation of the business occurs as a result of mishandling medical information.

## REFERENCES

Cate, F.H. (1997). *Privacy in the information age*. Washington, D.C.: Brookings Institution Press.

Cheng, V.S.Y., & Hung, P.C.K. (2006). Health insurance portability and accountability act (HIPAA) compliant access control model for web services. *International Journal of Healthcare Information Systems and Informatics*. 1(1), 22-39.

Culnan, M.J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*. September, 341-363.

Deshmukh, P., & Croasdell, D. (2005). HIPAA: Privacy and security in health care networks. In Peace, A.C., & Freeman, L. (2005). *Information ethics: Privacy and intellectual property*. Hershey: Information Science Publishing, 219-237.

Dhillon, G., & Moores, T.T. (2001). Internet privacy: Interpreting key issues. *Information Resources Management Journal*. 14(4), 33-37.

Institute of Medicine. (2001). *Crossing the quality chasm: A new health system for the 21<sup>st</sup> century*. National Academy Press: Washington, D.C.

Kaushal, R., Blumenthal, D., Poon, E.G., Ashish, K.J., Franz, C., Middleton, B., Glaser, J., Kuperman, G., Christino, M., Fernandopulle, R., Newhouse, J.P., Bates, D.W., and the Cost of National Health Information Network Working Group. (2005). The costs of a national health information network. Retrieved May 9, 2006 from the Annals of Internal Medicine website [www.annals.org/cgi/reprint/143/3/165.pdf](http://www.annals.org/cgi/reprint/143/3/165.pdf).

Kilman, D.G., & Forslund, D.W. (1997). An international collaboratory based on virtual patient records. *Communications of the ACM*. 40(8), 111-117.

King, W.R., & Epstein, B.J. (1976). Assessing the value of information. *Management Datamatics*. 5(4), 171-180.

Krzysztof, J.C., & Moore, J.C. (2002). Uniqueness of medical data mining. *Artificial Intelligence in Medicine*. 26(1/2),1-24.

Huston, T. (2001). Security issues for implementation of e-medical records. *Communications of the ACM*. 44(9), 89-94.

Landro, L. (2006). What drugs do you take? Hospitals seek to collect better data and prevent errors. *The Wall Street Journal*. May 23, D1.

Leach, S.L. (2004). Privacy lost with the touch of a keystroke? Retrieved March 23, 2005 from the Christian Science Monitor website [www.csmonitor.com/2004/1110/p15s02-stin.html](http://www.csmonitor.com/2004/1110/p15s02-stin.html) .

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*. 15(4), 336-355.

Office of Technology Assessment. (1993). Protecting privacy in computerized medical information. Retrieved August 6, 2006 from the Office of Technology Assessment Legacy website [www.wws.princeton.edu/ota/disk1/1993/9342/9342.pdf](http://www.wws.princeton.edu/ota/disk1/1993/9342/9342.pdf) .

Ogles, J. (2004). Court documents not fit for Web? Retrieved February 7, 2005 from the Wired Magazine website [www.wired.com/news/privacy/0,1848,65703,00.html](http://www.wired.com/news/privacy/0,1848,65703,00.html) .

Patton, S. (2005). Sharing data, saving lives. Retrieved July 27, 2006 from the CIO Magazine website [www.cio.com/archive/030105/healthcare.html](http://www.cio.com/archive/030105/healthcare.html).

Payton, F.C. (2003). Data mining in health care applications. In Wang, J. (Ed.), *Data mining: Opportunities and challenges*. Hershey: Idea Group Inc, 350-365.

Regalado, A. (2006). Plan to build children's DNA database raises concerns. *The Wall Street Journal*. June 7, B1f.

Rindfleisch, T.C. (1997). Privacy, information technology, and health care. *Communications of the ACM*. 40(8), 93-100.

Rubenstein, S. (2005). Next step toward digitized health records. *The Wall Street Journal*. May 9, B1f.

Saul, J.M. (2000). Legal policy and security issues in the handling of medical data. In Cios, K.J. (Ed.), *Medical data mining and knowledge discovery*. Heidelberg: Springer-Verlag, 17-31.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*. June, 167-196.

Straub, D.W., & Collins, R.W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly*. June, 143-156.

Warren, J., & Vara, V. (2006). New facebook features have members in an uproar. *The Wall Street Journal*. September 7, B1f.

Westin, A.F. (1967). *Privacy and freedom*. New York: Atheneum.

Wilson, J.F. (2006). Health insurance portability and accountability act privacy rule causes ongoing concerns among clinicians and researchers. *Annals of Internal Medicine*. 145(4), 313-316.

Yang, J.A., & Kombarakaran, F.A. (2006). A practitioner's response to the new health privacy regulations. *Health & Social Work*. 31(2), 129-136.

Yang, J.A., & Kombarakaran, F.A. (2000). Who knows your medical secrets? *Consumer Reports*. August, 22-26.

Yang, J.A., & Kombarakaran, F.A. (2006). The new threat to your medical privacy. *Consumer Reports*. March, 39-42.

