

# 13

## **Privacy and Technology in the Medical Field**

Nick Schuman and Chris Bixler

### **Introduction**

In October of 2004 West Palm Beach Police followed a lead in the investigation of two thousand painkillers written to the same patient in an unusually short time period. Their lead took them to the doctor's office of outspoken political journalist and well-known author, Rush Limbaugh. The sole purpose of their visit was to take the private medical records of Mr. Limbaugh and use them without his authorization in their investigation and prosecution.

Situations involving access to one's private medical information have become increasingly more common. The necessary privacy of this information is vital, easily compared to a social security or bank account number. Unfortunately, the majority of the population is not aware of the risks associated with the less than reliable security associated with the protection of medical records.

In 1996, the United States Government decided it was time to protect its citizens in regard to the invasion of medical records. The result was The Health Insurance Portability and Accountability Act (HIPAA) of 1996, which changed the security standard in the industry. Patients were now supposed to enjoy the benefits of a secure medical system, knowing that they had to sign a waiver in order for any third party to view their private medical information. Why then did Rush Limbaugh, a man all too familiar with his personal rights, appeal the unauthorized seizure of his medical records only to lose? In a medical industry working on digital standardization, citizens and patients alike need more than a governmental privacy act to truly protect the privacy of their medical information.

For years the standard in the medical field has been heavy, overfilled file cabinets leaking unorganized folders for the secretary to

fumble as one checks in for an appointment. Since the digital age, however, the medical field has moved along with most industries in a push towards digital standardization. Whether it is an online medical record database, a doctor's PDA, or electronically dispensed prescriptions, examples of technology are present everywhere in today's medical facilities.

One main effect technology has had on the medical field is the consolidation of medical records to a single digital file, thus allowing multiple parties access electronically to an individual's private medical records. Patients who receive treatment in multiple locations benefit from consolidated medical records, eliminating the valuable time and resources used in communication between different facilities. The downside to this consolidation is that it allows a person with the necessary skills access to private medical records through the invasion of integrated databases (2004 Freedman). Insurance companies, pharmaceutical companies, and medical websites are examples of standard entities that benefit from the collection and knowledge of individual and demographic personal information. However, in some extreme cases, medical information must also be protected from unauthorized viewing and seizure related to employment, hacking, government, and law enforcement. As one of the most important pieces of personal privacy, the protection of medical records is a complex and important issue concerning society.

When HIPAA was implemented in 1996, the medical field seemed to be moving in the correct direction concerning the privacy of patient medical records. According to a report in *Medical Verdicts and Law Weekly*, "One clear outcome of the implementation of the HIPAA privacy requirements was that it allowed facilities to address internal process issues that put privacy of patient information at risk" (LexisNexis Academic 2004). Although HIPAA has made some strides in the security of medical information, medical facilities agree that there are still several key areas for improvement. An important standard to begin with deals with the Health Information Management department present in all medical facilities. It is this department that is the only authorized party allowed to release any medical information for a patient. Other leaks of medical information, as small as height or weight data from a practicing physician, is considered a breach of HIPAA regulations (LexisNexis Academic 2004). Many patients do not realize this standard, and therefore contribute to the dilution of security present in many medical facilities. Other important areas for improvement include but are not limited to: standardized procedures concerning the authorized release of private patient information, obtaining protected health information from other providers, release of information to a patient's relatives or significant others, and business associates access to private medical records. These issues, while addressed under HIPAA, have still proven to be flawed and are in need of more secure measures. (LexisNexis Academic 2004)

There are also representatives from the other side of the medical field that feel medical privacy is a huge disadvantage to the cause that these medical specialists are trying to represent. These medical specialists represent the field of medical research, and the release of patient information, particularly deceased patients, is of the utmost

value in their ongoing efforts to understand medicine and the human body.

At the Annual Scientific Session of the American College of Cardiology, researchers from the University of Michigan Cardiovascular Center recently showed how HIPAA, the national medical privacy act, severely affected their ability to study heart attack patients after they left the hospital (LexisNexis Academic 2004).

Allowing medical records to fall into the hands of the appropriate research parties, with or without prior consent, is an issue that is widely debated from both sides. Relatives of deceased patients often feel it is a dishonor to the individual to commit the cadaver to the purpose of medical research, or even conduct an autopsy to study the cause and effects of a medical incident. Conversely, researchers argue that they cannot possibly continue to make sizeable progress in medical research without access to the records and remains of deceased patients with these various ailments. Even more extreme cases urge the fact that access to medical records could even save lives in the event of an emergency transfusion, trauma related accident, or infectious disease. In all cases there are two sides to the issue of medical privacy. Both arguments have valid points: one focuses on the benefits of the immediate patient while researchers target the issue of patients' lives saved in the future.

Compared to other secure information, medical information can actually be used in a positive and significant way even when it is gained in an unauthorized manner. Unauthorized access to a social security number or bank account number can easily be used maliciously when stolen, and can not be used for any benefit to the person it is taken from. Medical information can be used maliciously in many ways, but has the uniqueness of benefiting other patients through the study of various ailments. Unfortunately, patients are all too aware of the negatives of having medical histories fall into the wrong hands. There are a number of lawsuits over employers making decisions based on a predisposition to a various condition, and the employee not authorizing the viewing of his or her medical information.

Terri Seargent, a North Carolina resident, was fired from her job after being diagnosed with a genetic disorder that required expensive treatment. Three weeks before being fired, Terri was given a positive review and a raise. As such, she suspected that her employer, who is self insured, found out about her condition, and fired her to avoid the projected expenses (Weiss 2000).

Terri is just one of many examples of employees released from their jobs due to unauthorized viewing of her medical records from an employer. Another current and well-known example of medical privacy revolves around the nameless accuser in the Kobe Bryant rape case. In this situation, the accusers prior sexual activities were well known to the public, information that was gained through her medical records from the days preceding the alleged rape. Through the unauthorized release of her medical files from a hospital employee, observers could not argue that the girl had more than her share of sexual partners in the days before the alleged Kobe incident. The accusers asked the judge to discard the information citing the Medical Privacy Act as grounds for

dismissal. The case was eventually dropped from court, and it would be easy to come to the conclusion that this was because of the population's overwhelming knowledge of her private medical records.

It is easy to see the positive and negative effects of privacy in the medical field. However, it is not as easy to understand and find a common ground to which all parties are happy with the standard in the industry. Fully protected medical records leave medical researchers with less than satisfactory information to use, while unprotected information leaves loopholes for employers and legal entities to use against the patient. In an age of changing technology, where the medical file is being replaced with an electronic file on the doctor's PDA, or in the facility's online database, medical privacy is an issue that must be dealt with on a continuous basis. Standards in the industry change all the time, and cases involving medical privacy are often the fuel for change in the field. Patients and consumers alike need to be aware of their private medical information, those that have it, where it is stored, and the scenarios and situations that might arise if this information can be obtained without patient consent.

### **Medicine and Technology**

The medical field is comprised of such a complex group of individuals that there is a large range of opinions and beliefs concerning privacy and technology. To understand further the real life applications and situations concerning medical privacy and technology, a series of interviews were conducted with specialists each working in a different sector of medicine. From their comments, information, and opinions an understanding of the everyday implications of privacy in the field of medicine, and how technology is shaping these issues was gained.

**Technology Acceptance.** Governing all of the issues at hand was the underlying theme that medicine is behind other industries in the conversion towards the digital age and the acceptance of technology. As the field of medicine has advanced there have been many significant breakthroughs and inventions that shape the way medicine is performed today. Unfortunately, not all of these new ideas and technologies have been readily accepted by the majority of the field. There has always been a stubbornness and a certain unwillingness to change something that has been used or preformed for years. It is this problem which makes doctors uncertain when either accepting a new technology or moving their facility to an electronic system.

The slow acceptance of technology can partly be attributed to the way a doctor is trained to look at mistakes. Instead of examining the entire system or process for a mistake, most medical specialists approach medical mistakes from a personal blame standpoint.

Doctors are trained to make clinical decisions independently, without considering how their actions figure into a larger system of treatment, notes Tejal Gandhi, M.D., an associate physician at Brigham & Women's Hospital, Boston. "The concept of systems analysis doesn't come up," she said. Instead, doctors are mentored in an environment where "if you make a mistake, you feel like you are at fault," Dr. Gandhi said. This obviously contributes to a culture of blame and secrecy.

To overcome this, health providers need to get "desensitized" to the concept of medical errors, he said. "People have to get to the point that when you say you made a mistake, we think, what is wrong with the system instead of what is wrong with that person, said Dr. Leape, the coauthor of the March 18 special issue of the British Medical Journal on medical errors" (ahrq.gov 2004).

**Feasibility and Effectiveness.** Other than technology acceptance, some of the medical field has not converted to a digital system for other important reasons. Many specialists feel that the feasibility concerning a large scale installation and unification of electronic systems is very low. Combine this with the fact that many doctors feel the benefits are not clear, and technology becomes a difficult thing to implement in the medical field. Benefits, however, are exactly what these technologies do offer. Not only do electronic systems offer a huge savings in overhead costs, but the accuracy and privacy of patient medical records are increased exponentially. The feasibility is a concern, however, as combining medical records on a national level to integrate all electronic systems would be a massive, time consuming, and expensive project. Completing this huge task would be a giant step in the advancement of the medical field (Freedman 2004). Assuring that all doctors, no matter where on United States soil they are located, could quickly and accurately access a patient's medical information would be of incredible value. This would not only cut down the time needed to treat each patient, but also in emergency situations save lives.

To accomplish this project, medical facilities would have to start on a smaller scale by securely collecting and processing all of the hard copies of the medical records, and eventually scan them onto a digital version. Over a number of years, all of the nation's medical facilities could potentially have all files on an electronic medical record system, and completely end the use of paper records. The next step would be compiling these records into a national database, and consolidating duplicate patient information while adding information to build complete patient profiles. These national medical profiles would then serve as the future medical record for that individual, and all future additions and updates would be added electronically allowing all medical facilities to treat all of the nation's patients.

The ethical security and privacy issues that come along with this type of a system are very important, but aren't much more severe when dealing with an electronic system versus a paper copy. Theoretically, there would be ways of hacking into any electronic system, but the fact that all information would be encrypted makes an electronic system more secure than a cabinet full of medical files.

**Financial Barriers.** The last barrier to technological acceptance is the issue of finances. Health care providers have gotten more expensive, and tend to cover much less. In addition, the number of uninsured patients showing up at hospitals is ever growing, as many poor patients even turn to the emergency room for the regular practice medical issues (Schuman 2004). Overall, the health care system in the United States has become a problematic and an under funded system.

In the past four years, Americans have spent an ever-growing portion of their paychecks on health care and for the most part gotten less for their money, forcing millions into the ranks of the uninsured or personal bankruptcy, according to government figures and several independent assessments (Connolly 2004).

To solve these problems, and hopefully push the medical field in the right direction, hospitals have cut spending to improve products, processes, and services, fearing less government subsidization and reimbursements. In order to really get the field of medicine jumpstarted towards the digital age, the government would have to make a commitment to this industry, and begin to contribute financially to the success of the individual facilities. Without some kind of government backing, most hospitals fear the start up and training costs associated with widespread technological innovations. No one is sure what direction healthcare will move in, as we see more health issues each year, but less money for the field. This combination calls for a drastic change in the direction of healthcare, implementing a consolidated electronic system allowing fast, accurate, and successful patient treatment.

### **Employment**

Suppose an employer was deciding between two equally qualified candidates for a position within his company. The only difference between the two candidates was the fact that one of them has abnormally high levels of cholesterol, making him or her more susceptible to a future heart attack and being a future health care liability for the firm. The only reason the employer knows this is because he gained unauthorized access to the candidate's medical records. Through a series of surveys, questionnaires, and behavioral tests, employers can gain valuable medical information about candidates without ever viewing the physical medical file. In fact, according to workrights.org, there are a couple ways employers are gaining medical information about their future employees without "breaching" HIPAA. First, there has been a movement in increasing the sophistication of health tests, and second, there has been work done to better understand how lifestyles and behaviors are affecting a person's health (workrights.org 2004).

The first way employers are gaining valuable knowledge about their candidate's medical status is through more sophisticated testing. These tests include what on the surface look to be innocent questions about an individual's health history. Without even knowing it, a candidate may be eliminating him or herself from a job opportunity because they chose to reveal something about their medical past to an employer. Health questionnaires are not uncommon, in fact on the contrary:

A 1998 survey by the American Management Association, found that 49% of firms in the survey required medical examinations of all new hires. An additional 15% required medical examinations of new employees in selected job categories. For larger companies the percentage of employees tested was even higher -- 57% of companies with 1,000 or more employees required examinations of all new hires. Thus, roughly half of all U.S. employees are required to undergo pre-employment medical examinations (workrights.org 2004).

The second way employers are gaining employee medical information is through behavioral questioning. "Continuing scientific research has revealed numerous health problems related to common behaviors and lifestyles, including: smoking, obesity, diets high in fat, lack of exercise, and heavy drinking" (workrights.org 2004). An employer may choose to enquire on behalf of these issues. It is clearly up to the employee whether to give up this information or not, perhaps not understanding the implications behind answering truthfully.

Obviously, keeping medical history separate from a job application is imperative. Should medical records be obtained by an employer, it would be hard to argue against their reasoning to not want to take on the risk of heightening healthcare costs when others who are healthy are just as qualified.

### **Insurance**

The privacy of medical records needs to be defended even more when the topic of insurance is brought up. Insurance companies should only be privy to the knowledge a patient allows them to see. Obviously, health insurance companies are most likely going to be aware of the prescription drugs someone may be taking, as they are the ones most likely picking up most of the tab. However, giving too much information to an insurance company can only result in paying astronomical premiums or not being insured. For example, a car insurance company is going to take notice should they find out a person suffers from severe headaches with accompanying dizziness. While a person may not think revealing their problems with headaches could hurt them, an insurance company may believe the information warrants an increase in the risk they are taking by insuring a particular client, ultimately resulting in that person paying more.

### **Identity Theft**

The importance of keeping medical records private may actually have nothing to do with a person's medical history. Along with what prescription drugs one has been given by a doctor or what diseases one may carry, medical records also carry valuable information such as social security number, insurance provider, name, address, phone number, as well as the names of close relatives. Should this record fall into the wrong hands, not only can the person find out about a potentially negative medical condition, they can also take other information from the file and use it maliciously against the owner (Bixler 2004). Comparatively speaking, the damage of someone knowing about a negative ailment is far less than the damage caused by a person taking other information from a file. The financial reasons

alone associated with keeping a medical record private are reasons enough to defend medical privacy.

### **Problems with HIPAA**

The fact that the United States Government has acknowledged medical record privacy, especially the electronic variety, is a step in the right direction. However, the general consensus among professionals in the medical industry is that the Act does not really help anyone in medicine, and may actually impede in giving proper healthcare. In his interview when asked about HIPAA, Bernard Freedman, a physician, was quoted as saying:

HIPAA is a set of regulations originally promulgated to deal with electronic medical information only by a paranoid bureaucracy overly concerned with what 'Big Brother' might know about them. When the obvious fallacy of a difference between electronic and non-electronic information was pointed out, HIPAA was amended to include all medical records and information. It is a mistaken and misguided, poorly conceived and poorly implemented effort, which interferes on a regular basis with the necessary medical care of the individual. It is violated on a daily basis when a physician requests an x-ray, blood test, or advice of another medical professional without the prior written informed consent of the patient.

The industry believes that the government is going about medical privacy the wrong way with HIPAA. A better, more efficient way to deal with medical privacy is punishing the actions taken when medical information is disseminated, not punishing the dissemination of the medical information which is what HIPAA is currently doing. Technically, every time a nurse sees a file, a receptionist sets up an appointment, or a doctor asks another doctor a question about a situation, medical privacy is being breached. What needs to happen is when the information that is being talked about is used incorrectly, those actions should be punished, not the action of talking about a particular medical situation. Mr. Freedman went on to say that:

More or 'stronger' measures to protect our privacy in medicine would create even greater obstacles to better medical care. If there is a concern about any harm which might be done by the dissemination of such information, the law should provide for redress of any such harm proved to have been caused by the dissemination of that information.

While medical records should not be openly available for public viewing, the fact remains that medical privacy is technically being breached all the time. Therefore, Congress should rethink the act and focus more on the scenarios in which people are denied a job, promotion, or insurance due to an inquiry into someone's medical status.

## Medical Privacy Problems

The problems in health care concerning privacy and technology easily divide themselves up into several categories. Although there is much overlap in these problems, there exists a clear need for the reformation of HIPAA and overall medical privacy policies. The categories of medical privacy problems are: individuals getting exposed, unauthorized access, poor security, poor disposal, medical information used for marketing, government use of records, research, and law enforcement/lawsuits (healthprivacy.org 2004). In each of these categories there is a typical and frequent breach description easily showing the problems in that area.

When individuals are exposed, it usually revolves around their medical records becoming public without their prior authorization. As in the Kobe Bryant case discussed earlier in the chapter, publicized medical records can damage one's reputation, cause problems in the workplace, and even affect insurance rates. One incredibly terrible but interesting example concerned an Illinois woman and her post abortion medical records. Apparently, after some complications involving the operation, St. Elizabeth's Medical Center put her medical records on the Internet without her consent. She responded by suing the hospital, alleging that the hospital turned her medical records and a photo of her over to an anti-abortion activist website. She is also suing the anti-abortion group for invasion of privacy (healthprivacy.org 2004).

Unauthorized access is certainly one of the key contributors to individuals getting exposed. If only the correct people had access to medical records, a patient's privacy would be greatly increased. Unfortunately, it is difficult or impossible to create a foolproof system that nobody can breach. When unauthorized access is gained it is usually not the medical information itself the unauthorized party is after. Rather, they are breaching the system for other demographic information such as names, addresses, phone numbers, and social security numbers. It is often of value to even access a whole system and copy just the names and one other attribute to sell to various marketing entities. A common example of unauthorized access usually involves a hospital facility employee, or someone who has a reason to be on the system to begin with. "In 1994, a banker, who also served on his county's health board, cross-referenced customer accounts with patient information. He then decided to call due all mortgages of anyone suffering or diagnosed with cancer" (healthprivacy.org). Other common examples involve off duty hospital employees taking or downloading patient lists, stealing social security numbers for fraudulent activities, and collecting session records and notes.

Poor security is also a severe issue when dealing with the privacy of medical records in the age of newly emerging technologies. The reason most unauthorized access is gained is due to the poor security measures that have been the standard in the industry for years. Whether it is leaving a computer screen open while away from a desk, or simply having a patient file open on a counter, "HIPAA dictates that each facilities health information management (HIM) representative is the only one to communicate a patient's medical information" (hipaa.org 2004). Hospitals need to encrypt all the technology that they implement in their facility. Implementing these technologies eliminates the poor

security that comes along with the paper file and file cabinet. Without electronic medical records, it is too difficult to protect anyone's medical file and have any confidence that it is safe. Another common problem involves various online databases being linked to other sites containing confidential patient information:

At Drexel Medical School in Philadelphia, a hacker found a webpage used by the university that contained an open link to a database of neurosurgical patients. The database contained full demographic information, in addition to detailed notes on the diseases and treatments present (healthprivacy.org 2004).

The post-use disposal of medical information is an often overlooked but a very important aspect of patient medical privacy. Less important in the digital age, disposal of medical information must be secure and effective. The records must be retained for a set amount of time, after which they should be shredded if in paper form and securely maintained until the proper disposal service comes to discard them (Schuman 2004). When a facility is using an electronic system, records that are no longer needed or active should be erased on the computer so they can no longer be viewed by anyone at anytime. A very scary incident involving a poor disposal occurred when a hospital decided to upgrade to an electronic system. After moving several non-active medical files to a cabinet for storage, the hospital sold much of their storage equipment in the upgrade to EMR. Included in the sale was the cabinet full of files which was bought in 2002 by a man who noticed that all of the files included names and social security numbers of Medicaid patients (healthprivacy.org 2004).

Medical information can also be used for government and marketing purposes. Both marketing firms and the government can benefit by understanding various demographics, and having the ability to group certain types of people. This is not beneficial to the patient or consumer. By allowing either the government or marketing firms access to medical information one is giving up quite a large piece of privacy. Next thing one knows, ads for pharmaceuticals and other products begin appearing in the mail, on one's computer, and in other parts of everyday life. The products have been marketed because of some facet of medical information that placed an individual in a certain demographic group. Although there are times when marketing might be beneficial, it mostly works to bother and reduce an overall feeling of privacy.

In Florida in 2003 several residents were mailed packages of Prozac with a letter asking them to try it. Not only were the residents chosen at random from their addresses from local medical records, but few to none of them were in need of a mood and behavioral controller such as Prozac. Several receivers of the unsolicited Prozac filled privacy lawsuits against the involved parties (healthprivacy.org 2004).

### **Technologies and Future Possibilities**

It's no secret that the medical field has been behind in moving towards automating systems. With the advent of such things as EMR & PDA compatibility, the industry is showing signs of taking more advantage of the advances in technology. Adopting encrypted technology, while not completely safe, is much safer than the traditional paper & pencil approach to keeping medical files. The industry is behind, comparatively speaking, to other industries; however there are technologies available that help increase patient privacy. Some examples of the technologies that will help patient privacy are:

1. "ALARIS-Admin-Rx is a one-of-a-kind "smart pump" that provides bar code technology for intravenous medications. This technology can greatly help reduce patient and hospital mistakes by integrating correct medications with appropriate bar codes. By implementing bar codes, a patient's privacy can be further protected by the anonymity of the bar code. Instead of walking around with an IV with the label written on it for everyone to see, the label will be replaced with a bar code that needs scanning to determine what the IV's contents are."
2. "Connect-Rx is a Microsoft Windows NT-based medication management system architecture and family of solutions which automate the medication use process. Obviously, the fewer eyes that see a person's medical condition, the more the file is private. Anytime medical procedures such as management of medication use can be automated, privacy is increased and patient error is decreased (McKesson 2004).

3. An important idea to remember is the fact that technology can help reduce administrative error, especially with filling prescriptions. Automating the prescription process helps improve the accuracy of filling the correct prescription and it also improves patient privacy as a human is eliminated in the process. According to the McKesson Group in a seventeen-day study after implementing the ALARIS-Admin-Rx at the University of Wisconsin, medical error went down 87%. Among that statistic, wrong doses went down 100%, wrong administrative technique went down 100%, omitted doses went down 92% and the wrong timing of medicine release went down 77%. When this seventeen-day study was extrapolated to the year, the study shows that implementing this technology would result in 1,822 administrative errors per year as opposed to 13,340 errors if the technology were not adopted (McKesson 2004). Therefore, implementing this newer technology not only helps protect a patient's privacy, it seems as though it is essential in eliminating human errors.

### **Ethical Issues: Individual Versus Community**

There are severe ethical issues that come along with healthcare, privacy, and how technology impacts this field. At the forefront of these ethical dilemmas is the idea of individual benefit versus community benefit. This idea comes up quite frequently when dealing with medical privacy in terms of medical research, disease prevention and control, as well as dealing with a prominent figure's medical

conditions. The first issue, touched on briefly earlier in the chapter revolves around the potential medical research benefits that a reduction in privacy can create. Many relatives of deceased individuals chose to keep their loved ones intact, rather than committing their remains to the cause of medical research. On one hand it is the person's right to choose what happens to themselves or their loved ones after death, while on the other hand the benefits to the community in terms of disease research and treatment are huge. Understanding spiritual and personal beliefs is one of the things that unite this country in accepting a variety of personal practices. At the same time we are facing a time when new diseases are popping up everywhere, and medical researchers have trouble keeping up in terms of both time and resources. Allowing medical researchers unrestricted access to deceased patients with current problematic conditions would greatly reduce the time needed to find a treatment, and in turn, would isolate and destroy the disease before it can become a problem.

The other venue where disease becomes an ethical issue concerning the community versus the individual is if some kind of widespread disease did spread in this country. "In the next thirty years, we will likely see a disease that makes the Black Plague pale in comparison," says Professor Kai Larsen at the University of Colorado. How do we deal with this when the breakout first starts? Do we isolate and quarantine the individuals removing their rights to privacy? Do we also isolate anyone they have contacted within a certain time period so we reduce the degree of contagion?

In 1900, it was the responsibility of government agencies to identify sources of illness and isolate those people from others who might become affected. Aggressive programs to identify and sequester people who had tuberculosis were very effective in establishing control of this disease, which was the greatest single cause of death in 1900 in the U.S., and which had no known effective treatment. People were required by law to submit to testing for the disease (and health professionals still are). Once an affected person was identified, the law required evaluation and notification of all contacts of that person, and the person himself was sequestered from the rest of society, by force if necessary, to effect treatment such as it was, and prevent further spread of the disease (Freedman 2004).

Considering the severity of the results if we do not act, there must be measures put in place to handle a situation of this magnitude. Although it does strip citizens of some of their rights, it is more important to benefit the community in a situation with repercussions so severe. It is important to honor a person's privacy up to a certain point. If protection of privacy ends up meaning slow medical and disease research, or widespread disease, privacy cannot be accommodated. If the repercussions are not severe then it is important to maintain a person's privacy.

Privacy is a common issue to everyone in this world. Even celebrities are entitled to some degree of privacy, though they subconsciously agree to give up some of their privacy by appearing in

the spotlight. Both Kobe Bryant and Rush Limbaugh sacrificed a bit of their privacy by entering the public eye, but that doesn't mean they have no right to privacy. "During the Wilson Woodrow administration, our President was diagnosed with a severe condition that could result in death. He made the decision to keep this a secret from the American public and try to fight the disease while he served his term" (Freedman 2004). This choice serves the American public rather than the individual, unless the condition is affecting his performance.

There will never be a standard in the field of medicine as to what to report concerning patients. All too often people lie to themselves about their own condition, so they must not be honest with others. Healthcare needs to be reformed placing a balance ethically on community versus individual situations. Patients need their privacy protected, but not to the degree that it interferes with the advancement of medicine. Facilities need to implement technology to keep up with other industries. Researchers must find a balance between quicker development and patient privacy. The government must commit to health care, and business must respect the fragility of medical information. The sooner this is accomplished the sooner the medical industry will begin to see benefits both for the individual patients, as well as the United States as a whole.

### Works Cited

- Bir, Kate. Interview. 17.Oct 2004.
- Bixler, David. Interview. 18 Oct. 2004.
- Connolly, Ceci. "High Costs, Less Care." *The Washington Post*. 27 September. 2004. <<http://www.washingtonpost.com/wp-dyn/articles/A55301-2004Sep27.html>>.
- Freedman, Bernard. *Interview*. 17 Oct. 2004.
- "<http://www.hipaa.org>." *http://www.hipaa.org*. Fall 2004. HIPAA. 12 Oct. 2004.
- "Medical privacy law makes health research harder, more expensive." *Medical Device Law Weekly*. LexisNexis Academic. LexisNexis. 10 Oct. 2004 <<http://web.lexisnexis.com/universe/>>.
- "Medical Privacy Stories". *Health Privacy Project*. Oct 18, 2004. <http://www.healthprivacy.org>.
- "Organizations achieving HIPAA compliance, seeing positive results." *Medical Verdicts and Law Weekly*. LexisNexis Academic. LexisNexis. 10 Oct. 2004 <<http://web.lexisnexis.com/universe/>>.
- Schuman, Dorian. 18 Oct. 2004.
- Stein, Rob. "Implantable Medical ID Approved By FDA." *The Washington Post*. Oct 15, 2004.
- Tokarski, Cathy. "Medical error Prevention Strategies Face Barriers to Acceptance." <http://www.ahrq.gov/news/medscap2.htm>. Fall 2004. 8 Oct. 2004.
- Weiss, R. "Ignorance Undercuts Gene Tests' Potential," *The Washington Post*. December 2, 2000. Workrights.com. 29 Oct. 2004 <[http://www.workrights.org/issue\\_medical/mp\\_legislative\\_brief.html](http://www.workrights.org/issue_medical/mp_legislative_brief.html)>.