Ashley Rutherford

EH 121

Patient Privacy

As the computer, World Wide Web, and innovative technologies filter into almost every aspect of modern life, tangible paper documents have become obsolete to new high-speed data bases and online storage systems. The issue now becomes not how to develop and store these once dusty shelves of confidential files and folders, but how to keep them away from prying eyes. Because of restrictions under the Health Insurance Portability and Accountability Act (HIPAA) and the ease of which secure internet information can be accessed, patient medical records should not be placed on the internet; records should, instead, be stored on micro-silicon chips to ensure security.

Doctors are now using handheld devices, such as Personal Digital Assistants and laptop computers, to view and alter patient medical information. This poses an even greater threat to the security of the information since the electronic data being sent over a wireless device travels through the air, not through a telephone line or cable. Therefore, this allows the information to be picked up by unauthorized individuals if the right equipment is being used. Retrieval of such confidential information is in violation of HIPAA and has severe criminal penalties (Bernard 2).

Enacted in 1996, the Health Insurance Portability and Accountability Act was designed to protect individuals' rights to health insurance coverage during changes in their job or health status. HIPAA preempts state laws that undermine its privacy protections; however, state laws regulate the transfer of information if the laws are equal to or offer more protection than HIPAA (Parver 654). According to Conn, HIPAA is comprised of three main components-"promoting

electronic transmission standards for claims data, and regulating both the privacy of electronic medical records and the security of medical data storage and transmission"(26). The plan seeks to ensure that physicians, hospitals and insurance companies have safeguards in place to protect information and files from access by unauthorized persons or pharmaceutical marketing companies. However, many wireless systems do not comply with HIPAA regulations and are not equipped with proper security and firewalls, so the system is prone to hackers. Even personal e-mail must be encrypted under HIPAA guidelines; spam, pornography, and remote host content distributed by attackers compromises computers. This past year alone, the number of attempted by internet hackers has increased by 85% (Messmer 46).

While medical records provide basic information, such as name, address, social security number, etc., they also contain more personal data such as prescription medications, allergies, family history, X-rays, and insurance reports. "Some of the most sought-after information is that of patients who are members of preferred medical network plans"(Messmer 46). This information is then sold as credentials and made into counterfeit documents by criminals from Central and South America, who in turn sell the documents to illegal immigrants.

> What's to stop a hacker from breaking into one of these systems to steal personal information (such as social security numbers or other personal data)? And even if you've got a system that's harder to break into electronically than it is to get into Fort Knox with a pick and shovel, how do you know who's been looking at your private information? (Osterweil 73)

Onlookers may be individuals out to steal identities, insurance companies attempting to raise premiums, or simply teenagers trying to break the system. However, Messmer states that hospital and office employees are responsible for most security incidents, such as stolen laptops

and missing documents (14). Nevertheless, the risk of identity theft far exceeds the benefits of having effortless access to online medical information.

The need for backup electronic data began in September of 2001, when New York firefighters hurriedly grabbed markers to write their names and social security numbers on their arms before entering the World Trade Centers (Murray). As bodies were recovered, many were unidentified, while the remainders were still missing and unaccounted for. Mann relates the necessity of readily available data to Hurricane Katrina; doctors were faced with the impossible task of aiding the one million people whose medical records, like their lives, were destroyed by the storm. He suggests that patients need convenient access to their medical files, either in the form of paper documents, memory chips, or CD-ROMs, in the case of an emergency (Mann, 71).

This natural disaster represents the dire need for a nation-wide emergency management procedure in compliance with HIPAA regulations. During Hurricane Katrina, the Department of Health and Human Services issued a notice stating that "health care providers can share information to locate a patient's friends or family...the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others" ("Attitudes" 8). The Office for Civil Rights outlines permitted uses and disclosures when an individual's authorization is not required: "(1) to the individual, (2) treatment, payment, and health care operations, (3) opportunity to agree or object, (4) incidental use and disclosure, (5) public interest and benefit activities, and (6) research purposes or limited data sets" (4-5). The public interest and benefit activities section has several purposes; a patient's medical information can required by law, in the instance of court orders, subpoenas, government audits, crime evidence, or to report victims of abuse, violence, or neglect. The military also has the ability to demand medical records for the purpose of special missions or to conduct background

checks. Coroners, medical examiners, funeral directors, certain research groups, and other physicians are entitled to view a patient's health information without consent. The Food and Drug Administration may even obtain information for product studies, recalls, and marketing ("Summary" 7).

While the Department of Health and Human Services may have had good intentions, their issued statement throws into question the extent to which HIPAA and confidentiality should be enforced. Ethical issues became blurred under section five of the outline; for instance, doctors did not hesitate to discuss patient information in front of photographers and news reporters, who then used the information in articles and reports rather than to help locate family members. This information was released freely to the media without permission from the patient. Some hospitals even created online directories modeled after the patient locator website initiated by the Greater New York Hospital Association following September 11th. The site allowed the public to enter in names and receive basic information about the people they were attempting to locate ("Attitudes" 9).

Since then, Congress has established a central emergency system of public health preparedness and health information privacy. Only a national officer or state's governor, not local officials, has the authority to declare a public health emergency. In doing so, the governor may claim property, suspend bylaws, impose vaccinations, or quarantine individuals. HIPAA also permits several exceptions where disclosure to personal health information without patient authorization is allowed; however, this is based on a "good faith requirement."

The Secretary of Health and Human Services issued public health emergency declarations for five Gulf coast states.

> Included within the declarations were waivers of certain HIPAA privacy provisions. Penalties for noncompliance were waived regarding the need to obtain a patient's consent prior to speaking with family members or friends, or the desire not to be published in the hospital's directory. In addition, requirements for notification of privacy practices and the patient's right to ask for restrictions on his or her privacy rights also were waived (Parver 660).

This HIPAA waiver only remained effective for three days because medical ethics councils recognized the declaration's violation of the "good faith requirement."

A "good faith requirement" simply means that HIPAA can be broken with the understanding that by doing so, the individual, his or her family, and their private information will be released at a minimal level. Only enough information will be revealed as to inform the general public (Parver 655). For instance, if medical professionals treat an individual with Avian Flu, it is their responsibility, under the Model State Emergency Health Powers Act, to inform the government and the media. In doing so, they may release information about the case such as symptoms, how quickly the disease can progress, the side effects, treatments, etc, however, they may not release a patient's name, picture, medical history, or other personal information without consent. As evident during Hurricane Katrina, this "good faith requirement" was forgotten. Media organizations released more than the necessary amount of information on patients needed to inform the public. A fine line must be drawn between an individual's privacy and the public's need for information.

A practical solution to the portability and privacy dilemma is the technological VeriChip or RFID (radio frequency identification device) tag. Applied Digital Technologies, based in Palm Beach, Florida, created a microchip that can store a wide variety of data ranging from

several bytes to several gigabytes of data, making it a small, yet efficient answer to electronic storage. VeriChip tags are made with a type of silicon that can last up to 20 years, and the chip costs around $200. This new technology is more efficient than fingerprint biometrics and can always be removed (Streitfeld). "The RFID technology has been around for years; similar devices track products through the supply chain in many industries" (Gaudio 16). Such chips have already been used in household pets, such as dogs and cats; the chip contains an uplink to a global positioning satellite, which then relays a pet's position and status to the company and owner. The United States Government has also been using such a device for over ten years to monitor the location and condition of special military personnel and secret service operations (Gibson 50). More recently, the chips were marketed to Alzheimer patients and those with detailed medical histories, and the tag has been a success with senior adults and there is currently a waiting list of approximately 5,000 people (Streitfield).

Surprisingly, thousands of sales have been outside of the United States. Mexican officials have undergone implantation as a security precaution (Murray 1). Central American governments have persuaded parents to tag their children in order to identify them in the case of a kidnapping. In contrast, Spain has taken the chip outside of the medical world and uses the technology in electronic billfolds that act as banking cards to make purchases (Kanellos).

As stated by Murray, the RFID chip has been proven compatible with human tissue, allowing it to be used in artificial joint reconstruction, pacemakers, and defibrillators. Because of the chip's size, 11 millimeters, it can be implanted through a syringe into fatty tissue, usually below the right tricep or arm (Kanellos). Approved by the Food and Drug Administration, the VeriChip allows for effortless storage of secure medical records that would always be on the patient and easily accessed by authorized personnel.

Once a patient entered a hospital, they would be scanned, and within seconds their medical history, allergies, medications, and information would be displayed on a screen. The VeriChip transmits data through an electromagnetic coil equipped with a tuning capacitor, and the unit is activated by moving a scanner within a foot of the chip. The scanner charges the coil and activates the chip, permitting it to transfer data (Murray). The VeriChip scanner reads a 16-digit code, which opens an online emergency health record. Zillwich states that over 98,000 Americans die each year because of medical errors, inaccurate prescription dosages, and other treatment mistakes (1). Because information can be easily accessed, correct diagnoses can be made and treatments can be administered quickly without the need for unnecessary and expensive medical tests and procedures, thus saving money and valuable time (Gaudio 15).

After the data has been reviewed and updated, the information on screen would go away, leaving the new information on the chip in the patient. Applied Digital representatives say that security and privacy are not a concern because the chip does not emit a signal and can only be read from a maximum distance of three feet. Many physicians praise then new chip, saying that it eliminates much of the hassle of being on-call and reduces the time it would have taken to go to the office, find the chart, and then go to the hospital. Still other medical personnel are eager to see VeriChip used in pacemakers and artificial hips and knees. The chip's electronic code could store the implant's serial number, data on the implant manufacturer, the date of last battery change, the amount of battery life remaining, as well as which hospital staff members performed the operation (Murray 1).

The twenty-first century has ushered in many new technological innovations and responsibilities, with those comes the necessity for portable medical records via electronic data. With so many doctors using wireless technology in their day to day activities, the proper security

will be very important in order to protect patient information and any other data that is considered private by the HIPAA standards. Considering the danger of online personal information and the strict regulations of HIPAA, VeriChip is the best alternative to secure, reliable, electronic data storage and maintenance.

Works Cited

"Attitudes Toward Privacy Rules May Change in Times of Disaster." News Media & the Law 31.1 (Winter 2007): 8-9. Academic Search Complete. EBSCO. Dupont-Ball Library. 20 Nov. 2008 <http://search.ebsco.com/login.aspx?direct=true&db=a9h&AN=24737171&site=ehost-live>.

Bernard, Dornbrand, et al. "HIPAA and Patient Care: The Role of Professional Judgment." Journal of American Medicine 293.14 (2005) 1766-1771.

Conn, Joseph. "HIPAA, 10 Years After." Modern Healthcare 7 Aug. 2006: 26-28

Gaudio, Thomas. "A Chip in Every Arm, A Reader in Every Emergency Room." Njbiz 19.42 (16 Oct. 2006): 15-17. Regional Business News. EBSCO. Dupont-Ball Library. 24 Nov. 2008 <http://search.ebscohost.com/login.aspx?direct=true&bd=bwh&AN=22843146&site=ehost-live>.

Gibson, William. "Will We Plug Computers Into Our Brains? (Cover Story)." Time Europe 156.1 (03 July 2000): 50. Academic Search Complete. EBSCO. Dupont-Ball Library. 24 Nov. 2008 <http://search.ebscohost.com/login.aspx?direct=true&bd=a9h&AN=3322767&site=ehost-live>.

Kanellos, Michael. "RFID Chips Headed for Hospitals?" Silicon.com. 28 July 2004. Sony. 19 April 2007 <http://hardware.silicon.com/storage/0,39024649,39122659,00.htm>.

Mann, Denise. "Katrina Shows Need for Electronic Health Records." National Youth Leadership Forum Journal on Medicine 14(2006): 71-72.

Messmer, Ellen. "Healthcare Organizations Feel Security Pinch." Network World 25.9 (03 Mar. 2008):14-46. Business Source Premier. EBSCO. Dupont-Ball Library.

20 Nov. 2008 <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=31285640&site=ehost-live>.

Murray, Charles. "Injectible Chip Opens Door to 'Human Bar Code'." EETimes 4 Jan. 2002 1-5. 19 Apr. 2007 <http://www.eetimes.com/story/OEG20020104S0044>.

Osterweil, Neil. "Electronic Records, Private Lives." National Youth Leadership Forum Journal on Medicine 16(2006): 73-74.

Parver, Corrine. "Lessons from Disaster: HIPAA, Medicaid, and Privacy Issues- The Nation's Response to Hurricane Katrina." Administrative Law Review 58.3 (Summer 2006): 651-62.

Streitfeld, David. "Chip Implants in Humans Begin Today." EmergingWorlds.com. 10 May 2002. Los Angeles Times. 19 April 2007 <http://www.emergingworlds.com/mc_article.cfm?link=Chip_implants_in_humans_begin_today>.

"Summary of the HIPAA Privacy Rule." Office for Civil Rights. May 2003. United States Department of Health and Human Services. 20 Nov. 2008 <http://www.hhs.gov/ocr/privacysummary.pdf>.

Zwillich, Todd. "Government Moves to Expand E-Medical Records." WebMD.com. 2005. WebMD, Inc. 20 Nov. 2008 < http://www.webmd.com/news/20051006/government-moves-to-expand-e-medical-records>.