Proceedings of the 28th IEEE
EMBS Annual International Conference
New York City, USA, Aug 30-Sept 3, 2006

Security and Privacy Issues with Health Care Information Technology

Marci Meingast, Tanya Roosta, Shankar Sastry
Department of Electrical Engineering and Computer Sciences
University of California, Berkeley, CA, 94720
{marci, roosta, sastry}@eecs.berkeley.edu

Abstract— **The face of health care is changing as new technologies are being incorporated into the existing infrastructure. Electronic Patient Records and sensor networks for in-home patient monitoring are at the current forefront of new technologies. Paper-based patient records are being put in electronic format enabling patients to access their records via the Internet. Remote patient monitoring is becoming more feasible as specialized sensors can be placed inside homes. The combination of these technologies will improve the quality of health care by making it more personalized and reducing costs and medical errors. While there are benefits to technologies, associated privacy and security issues need to be analyzed to make these systems socially acceptable. In this paper we explore the privacy and security implications of these next-generation health care technologies. We describe existing methods for handling issues as well as discussing which issues need further consideration.**

I. INTRODUCTION

The health care system has long been plagued by problems such as diagnoses being written illegibly on paper, doctors not being able to easily access patient information, and limitations on time, space, and personnel for monitoring patients. With advancements in technology, opportunities exist to improve the current state of health care to minimize some of these problems and provide more personalized service. For example, the embracing of the Internet by health care organizations in the last decade has provided a medium for publishing general health information allowing patients to gain more knowledge about medical conditions. Currently, more than 90% of the approximately 5000 member institutions of the American Hospital Association reported having web sites, with most having descriptive information about their facilities and services.

Many technologies are currently being adopted by the medical field. In this paper we look at the move towards Electronic Patient Records(EPR) and the use of sensor networks for remote patient monitoring. With health care organizations transitioning to EPRs, information that was once stored in paper format will now be stored electronically allowing for easy accessibility and use. Aiding this transition, IEEE has joined forces with the American Medical Association and eight other major nonprofit medical and engineering societies to form an umbrella consortium, the Biotechnology Council [1]. The council's primary goal is to standardize everything from medical terminology to networking protocols so that medical records can be stored electronically and be instantly sent anywhere in the world.

In order to communicate the data in EPRs, a relatively small, but ever increasing percentage of health care groups have created 'web portals' that provide personalized patient services via the web. The "MyHealth@Vanderbilt" patient portal [15] and "Patient-Centered Access to Secure Systems Online (PCASSO)" at University of California, San Diego [9] are just some examples of developing advanced health care sites. These sites provide a set of individualized services to allow patients access to their clinical laboratory results and other components of the electronic patient records. These services have previously been available only to physicians and other health care providers.

Sensor network is another technology that is being adopted. Both industry and academic institutions are developing sensor systems for remote patient monitoring. For example, Intel's Integrated Digital Hospital (IDH) is aimed at improving health care worldwide by linking people, processes and technologies [17]. The IDH system combines mobile point-of-care (MPOC) and other information technology to integrate patient and administrative information into a comprehensive, digital view of a patient's health. The Information Technology for Assisted Living at Home (ITALH) project at University of California, Berkeley is looking at sensor networks for remote patient monitoring [6]. This project aims to create a system based on wearable sensors that will allow people who require assistance to live at home to do so using information technology. Kansas State University and the University of Alabama in Huntsville have a combined effort working on Wide Area Body Networks (WABN) Infrastructures [12].They are developing wearable health status monitoring systems that can be used for in home patient monitoring.

These technologies will provide many benefits for health care delivery, yet there are a number of security and privacy implications that must be explored in order to promote and maintain fundamental medical ethical principles and social expectations. These issues include access rights to data, how and when data is stored, security of data transfer, data analysis rights, and the governing policies. While there are current regulations for medical data, these must be re-evaluated as an adaption of new technology changes how health care delivery is done.

In this paper we explore the security and privacy is-

This work was supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Qualcomm, Pirelli, Sun and Symantec.

sues surrounding electronic health care records with patient portals and remote sensor networks for patient monitoring. In section 2, we provide some basic background on these systems and what standards are currently being used. We explore the security and privacy issues surrounding how the medical data will be used and transmitted in these systems and the current regulatory system for health care data in section 3. Section 4 discusses existing solutions as well as what future work needs to be done to make the systems more secure and eliminate the privacy concerns. We conclude in section 5 with a summary and recommendations.

II. Technical Background

Sensor networks for remote patient monitoring and EPRs take advantage of the existing technologies, such as the Internet and wireless communication. We describe the technical implementation of these systems in order to motivate the discussion of security and privacy concerns.

A. Electronic Patient Records

Electronic patient records take the current paper-based documents and convert them to a digital format so they are available electronically. The records include different types of data, such as physician's notes, MRIs, and clinical lab results. Using EPRs allows real-time access to health care records independent of the physical location of the user. Physicians, nurses, insurance companies, and patients can all access the records over the Internet. EPRs reduce the number of errors due to illegibility, and inconsistency of terms. In addition, electronic records can be backed up more easily than paper-based records which prevents data loss [10],[1].

The implementation of EPRs includes a local data base that collects all the information for records of patients at a certain location. For example, each hospital may have its own electronic database of patient information. These local data bases can then be connected via the Internet for data transmission so that a doctor at one hospital may view a patient's information from another hospital. Using the Internet and interfaces designed for presenting these records, such as the patient portal at Vanderbilt and PCASSO, a patient's data can be transmitted to physicians, the patient at home, and other health care providers.

B. In-home Remote Patient Monitoring

With the evolution of sensor networks, real-time in-home patient monitoring is more feasible. Figure 1 shows the overall remote patient monitoring system. Different types of sensors can be used at home to monitor a patient's vital signs. Wearable devices, such as electrocardiogram sensors and pulse oximeters, are being used along with non-wearable ambient temperature and humidity sensors. New sensors are also being developed to do different forms of monitoring. For example, wearable fall detectors that include accelerometers are being developed by ITALH [2].

In most of these systems, a periodic report from the sensors is sent back via wireless communication, using ZigBee, Bluetooth, or other technologies, to a local base station within the home. This local base station, e.g. a personal computer, evaluates the data sent back by the sensors. For example, if data of an abnormality in vital signs appears, the local base station can send the sensor data, along with an alarm, to a central monitoring station. This enables the health care providers at the central monitoring station to take the appropriate steps to aid the patient. The transmission of the information between the home and the monitoring site is done through the Internet. This type of system minimally restricts the patients daily activities, while still allowing him/her to be monitored.

C. An Integrated System

In order to get the most benefit out of these technologies, the two systems can be integrated. Once sensor data is transmitted to the central monitoring station, it can be incorporated into the patient's EPR. This information can be used to aid in better health care delivery by giving a more detailed description of the patient's medical situation.

III. PRIVACY AND SECURITY ISSUES

While the above mentioned technologies can help improve overall quality of health care delivery, the benefits of these technologies must be balanced with the privacy and security concerns of the user. Data from in-home sensors and medical records will be communicated electronically via the Internet and wireless transmissions. This increases the danger of compromising the security and privacy of individuals which we analyze in this section.

A. Data Access and Storage

There has long been concern over a patient's health record privacy and confidentiality [5]. Connecting personal health information to the Internet exposes this data to more hostile attacks compared to the paper-based medical records. Currently, patients have to physically go into a health care facility to get their medical record. Since the records are in paper format, this physically limits the number of people who see the record and how it gets transmitted.

However, once this information is available electronically, it opens the door for hackers and other malicious attackers to access the records as well as those who are authorized. In addition, given the distributed nature of sensor networks for in-home patient monitoring, there is a greater challenge in ensuring data security and integrity compared to the traditional health care system. Eavesdropping and skimming are a possibility when the sensor data is transmitted wirelessly. Data access, storage, and integrity are key challenges when implementing EPRs and in-home sensor networks.

In order to deal with the challenges of electronic data and remote transmission of the information, the following questions need to be answered:

- **Who owns the data?** Who has the authority to delete, edit, and add information to health data as well as enforce regulations surrounding it? Do individual patients own data collected on themselves? Do their physicians own the data? Do their insurance providers

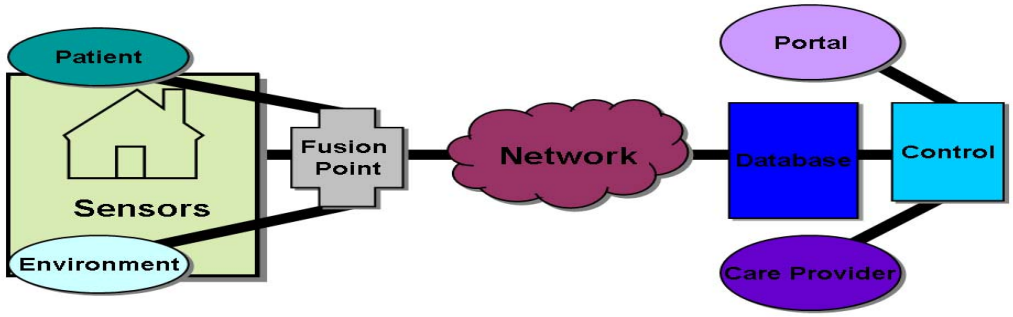

Fig. 1. The remote patient monitoring system.

own the data? Are they all joint owners? The question of 'who owns the data' is particularly troublesome and unsettled.It has been the object of recurrent, highly-publicized lawsuits and congressional inquiries. Furthermore, some HMOs have been refusing to cover a patient's expenses when the patient has participated in clinical treatment protocols that are experimental [3]. This bring up the question that if the insurance provider does not own the patient's data, can they then refuse to pay for expenses associated with the collection and storage of the data? This question in turn affects third party rights. If data is passed to a third party, do they have the same authority as the data owner, or are their rights more narrow? It is unclear what level of privacy and security protection must be maintained when data is transferred to a third party.

- **What type of data, and how much data, should be stored?** Doctors' notes, MRIs, and lab test results are examples of data that is stored in patient's paper-based record. Regarding EPRs, should all of this data be electronically stored or will a subset of this data be sufficient for health care purposes? For example, data may be aggregated and the results stored, and this may be enough information for the EPR users. This question also applies to the case of remote patient monitoring using sensor networks. For example, should the bulk of the raw data be stored locally at the patient's residence, while only the aggregated data required for diagnosis and emergency response is transmitted back to the monitoring center? The amount of sensor data that is stored in the central location needs to be just enough to accomplish the tasks related to the patient care. Any extra information will not have a significant impact on patient care, but may further compromise the individual's privacy. In both cases the granularity of data collected and stored needs to be minimized as much as possible while still achieving the desired level of health care.
- **Where should the health data be stored?** This is a question of centralized versus decentralized storage. In the case of EPRs, should data reside in local databases that can be connected to each other, or should it be stored in a central database? In the case of remote patient monitoring, should the raw sensor data be stored only locally or should it also be stored at the central monitoring station? What type of data storage will best accommodate the privacy and security needs?
- **Who can view a patient's medical record?** We divide the EPR users into two categories: a) users with the read/write privileges - such as the doctors and nurses, who can not only view a patient's EPR, but can also edit the records. b) users with read only privileges - for example, the insurance provider might be limited to only viewing the patient's EPR, but can not edit it. Depending on which user is accessing the EPR, there might be further restrictions on which portions of the data their privileges apply to. For example, in the case of an insurance provider, their access might be limited to the part of the EPR which facilitates the reimbursement for medical expenses. In another example, an elderly patient might want to authorize partial viewing of his/her medical record to certain relatives.
- **To whom should this information be disclosed to without the patient's consent?** There are situations in which the patient's health information needs to be disclosed to people other than the previously authorized users. For example, in the case of remote patient monitoring, an emergency might necessitate disclosure of health data without the patient's consent in order for that patient to receive necessary care.

B. Data Mining

Data mining is the process of analyzing data to identify patterns and/or relationships. Human medical data is seen to be one of the more rewarding and yet most difficult of all biological data to mine and analyze. Data mining on human subjects can provide observations that cannot be gained or easily extrapolated from animal studies. Visual and auditory sensations, the perception of pain, discomfort, and other reaction can be hard to learn from tests on animals [3]. However, when mining on human data, there are unique privacy and security constraints that limit what collection, distribution, and analysis can be done.

Currently, large amounts of medical data is not stored electronically and cannot be mined. Yet there are still thousands of terabytes of electronic human data generated annually in North America and Europe. While the type of data mining done on this information has security and privacy concerns, the heterogeneity of the databases and the scattering of the data throughout the medical care facilities without any common format or principles of organization, restrict what can be done. As EPRs become widespread, more health organizations will have databases which store patient information in a common computerized format. This data can then be easily shared over the communication network which will create a larger source of human medical data. Given this increase in available data, the role of data mining and how it is governed needs to be assessed.

From mining on medical data, one may be able to categorize and profile patients based on numerous factors such as age, gender,or disease. This may lead to discriminatory and exclusionary effects. As this data becomes a more of a ”commodity” that can be passed over the Internet and collected, it is important that anonymity of data happens before any data mining takes place. The question of what anonymity entails and regulations for data disclosures to users, such as managed care evaluators and insurance companies, all must be answered in terms of data mining.

Anonymizing data can happen on multiple levels. For example, removing personal identifiers such as name, age, and social security number may make it hard to link data up to a unique individual. However, even this may not make the data anonymous enough to prevent discriminatory effects. The data, while not correlated to a unique individual, may be able to be linked to a larger sub-population, such as people who live in a specific geographic region or people of a certain gender/race. What the appropriate level of anonymity is for a given data mining task must therefore be evaluated.

This leads to the question of who should have access to the data and at what level of anonymity. The information from a PC for at home patient monitoring may send the data to the hospital with some identifying tag on it to signal what patient the data is coming from. The physician needs to know who the patient is and may need to do some mining on the data over time, but does the insurance provider? What level of knowledge do different providers get? What level of data mining capabilities should different providers be allowed? Ethical practices are not well defined for the vast array of disclosures to secondary users, such as managed care evaluators and insurance companies[1].

These issues surrounding data mining need to be evaluated and regulations put in place to maximize the benefits from having more medical data readily available, while minimizing harmful effects.

C. Conflicting Regulatory Framework

There are currently many different regulations and rules surrounding health care including the Federal Regulations of The American Health Insurance Portability and Accountability Act(HIPAA) as well as various state regulations. While these regulations provide a framework of policy, they will have to be adapted as EPRs and sensors change the way health care is delivered.

HIPAA is a set of rules to be followed by doctors, hospitals and other health care providers. HIPAA's goal is to ensure that all medical records, medical billing, and patient accounts meet certain consistent standards with regards to documentation, handling and privacy. Moreover, HIPAA requires that all patients be able to access their own medical records, correct errors or omissions, and be informed how their personal information is shared or used. Other provisions of HIPAA include notification of privacy procedures to the patients [14].

At the same time, each state has specialized rules for how health care is handled, which are nicely described by the Health Privacy Project's *The State of Health Privacy*[13] . For example, the Alabama Code has no general statute granting patients the right to access their own medical records. It also does not have a general statute restricting the disclosure of confidential information. However, regarding certain medical conditions, such as mental health disorders and sexually transmitted diseases, Alabama has some statutes that control a patient's access to information as well as disclosure of this information. Alabama Code also restricts disclosures of medical information by HMOs. In contrast, California statutes grant patients the right of access to their health care information from health care providers, HMOs, insurers, and state agencies. California Code also has extensive regulations on disclosure and use of health care information by these entities.

There is a need to have cohesive policies to protect sensitive personal health information as it becomes available electronically. With the varying state codes there are uncertainties in data ownership, access rights, and disclosure as data may gets passed across state lines electronically. The HIPAA Privacy Protection mandates from 2003 are a foundation for a national standard for health privacy [14]. However, they are a minimum set of rules. They are a 'baseline' with minimum protections for consumers with stronger or more stringent state laws still remaining in effect. States are also free to enact stronger protections in the future.

As an example, under the HIPAA Privacy Protection rules, no consent is necessary by the patient for one doctor's office

[1]Primary users refers to patients, physicians, nurses, and other clinicians.

to transfer a patient's medical records to another doctor's office for treatment purposes. If the state laws governing disclosure and use of this information are more stringent in the patient's home state than the state the record is transferred to, the patient might have security and privacy expectations that may not be upheld. While this can happen with paper based medical information, the move toward electronic medical data increases the ease and amount of data which can be transferred across states.

IV. SOLUTIONS

In this section we discuss the existing solutions as well as open research questions regarding these privacy and security concerns.

A. Existing Solutions

The issues of data access, storage, and analysis are not unique to the medical arena. These problems have been looked an in a number of areas, from financial services to internet shopping, and technical solutions exist which can be applied to health care to increase privacy and security in a multi-user setting:

- **Role-based access control:** one of the most challenging problems in managing large networks is the complexity of security administration [16]. Role based access control, or role based security, is the dominant model for advanced access control. It results in the reduction of the complexity and cost of security administration in large networked applications. An example of role based access control for health care is in [7].
- **Encryption:** Encryption can be used to ensure the security of the data and help prevent eavesdropping and skimming. Encryption can be accomplished in hardware as well as in software. In order to ensure the highest level of security, it is best if both forms of encryption are used. Different symmetric and asymmetric key algorithms can be used to provide encryption in software [11]. In sensor networks, TinySec [8] is specifically designed to provide encryption and authentication capabilities. TinySec is already employed by some medical sensor systems such as the Kansas State University/University of Alabama in Huntsville WBAN.
- **Authentication Mechanisms:** Authentication mechanisms can be used to ensure the data is coming from the person/entity it is claiming to be from [11]. There has been a number of authentication algorithms developed such as passwords, digital signatures, and challenge-response authentication protocol. There are methods designed for sensor networks that are more energy efficient, such as the hash function in TinySec, that can be used for authentication.

B. Future Work

While there are methods that can be employed to aid in security and privacy of medical data with these new technologies, there are still areas that can be improved upon.

- **Define clear attributes for role based access:** Clear rules for the role-based access need to be defined so that these systems can be put in place. These can be dynamic rules or static rules depending on what is appropriate.
- **Policy development:** New policy needs to be created that can deal with across state jurisdiction. While the HIPAA Privacy Rules provide some groundwork, more needs to be done to create clear rules that users can rely upon. The move toward EPRs and the increasing amount of medical data that will be gathered due to remote sensor networks, creates the ability to transfer large amounts of data quickly. This necessitates a comprehensive set of regulations that protect a user's privacy and security independent of which state the data is located in. In the current setting many patients are not sure about their privacy rights regarding medical data and are ill-informed. As more medical data becomes electronic and can be easily transmitted, this will magnify the confusion of users unless clear guidelines are defined.
- **Rules on patients privacy at home:** Can the patient have full control over how much of the data is sent to the central monitoring station, or does the patient only have partial control? Guidelines need to be drawn which will regulate what sensor data collection entails and who will have control over it.
- **Data mining rules and technological measures:** These include not only who has the right to analyze what type of data, but also include the rules on anonymizing the collected data. The appropriate technical methods for ensuring these rules then need to be put in place if some form of automation is possible.

V. CONCLUSION

Technology is enabling medical health records to be put in the electronic format, EPRs, and making them available to the users via the Internet. In addition, advances in the area of sensor networks are making the idea of remote patient monitoring a reality. In this paper we discussed the privacy and security issues that arise when integrating these new technology into the traditional health care system. We explored some of the existing solutions that can be employed and the open research questions that need to be answered before the widespread use of the new technology is possible with minimal security and privacy risks.

REFERENCES

[1] Trudy E. Bell, *Medical Records: From Clipboard To Point-and-Click*,The Institute, December 2006.

[2] Garrett Brown, *An Accelerometer Based Fall Detector: Development, Experimentation, and Analysis*, Internal Report, University of California at Berkeley, July 2005.

[3] K.J. Cios and G.W. Moore, *Uniqueness of Medical Data Mining*, Artificial Intelligence in Medicine Journal, 2002.

[4] Computer Science and Telecommunications Board, National Research Council, *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academy Pr; 1997.

[5] Computer Science and Telecommunications Board, *Networking Health: Prescriptions for the Internet*,2000.

[6] J. Mikael Eklund, Thomas Riisgaard Hansen, Jonathan Sprinkle and Shankar Sastry, *Information Technology for Assisted Living at Home: building a wireless infrastructure for assisted living*, EMBC 2005, Shanghai China, September, 2005.
[7] M. Evered, S. Bogeholz, *A Case Study in Access Control Requirements for a Health Information System*, Australasian Information Security Workshop, 2004.
[8] C. Karlof, N. Sastry, and D. Wagner, *TinySec: A Link Layer Security Architecture for Wireless Sensor Networks*, Conference on Embedded Networked Sensor Systems, 2004).
[9] D. Masys, D. Baker, A. Butros , K.E. Cowles, *Giving patients access to their medical records via the internet: the PCASSO experience*, Journal of American Medical Informatics Association, 2002 Mar-Apr; 9(2):181-91.
[10] Simon Rogerson, *Electronic Patient Records*,IMIS Journal Volume 10,No. 5, October, 2000.
[11] Serge Vaudenay, *A Classical Introduction to Cryptography : Applications for Communications Security*, Springer, 2006.
[12] S. Warren, J. Lebak , J. Yao , J. Creekmore , A. Milenkovic , and E. Jovanov, *Interoperability and Security in Wireless Body Area Network Infrastructures*, EMBC, Shanghai China, September 2005.
[13] *Health Privacy Project* at www.healthprivacy.org/info-url_nocat2304info-url_nocat.htm
[14] *HIPAA 101.com - Info Guide to HIPAA Compliance, Implementation and Privacy* at www.hipaa-101.com
[15] *MyHealthAtVanderbilt* at www.MyHealthatVanderbilt.com
[16] *Role Based Access Control* at http://csrc.nist.gov/rbac
[17] *Solutions for Improving Healthcare* at http://www.intel.com/business/bss/industry/healthcare/index.htm