**Master’s Project Proposal**

**PERSONAL PRIVACY POLICY CONTROL SYSTEM IN ELECTRONIC HEALTH RECORDS**

Project Report submitted to

The Department of Computer Science

New Jersey Institute of Technology.

# In Partial fulfillment of the requirements of the Degree of Master of Science in Computer Science

Submitted by: **Pratik Hatkar**

NJIT id**: 217 65 117**

email **: pvh3@njit.edu**

APPROVALS

Proposal Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Agree to Advise: \_\_**Prof. James Geller**\_\_\_\_\_\_\_\_\_\_\_\_

(Project Advisor)

Date Submitted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(MS in CS Committee)

Date Approved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract**

For many years, health care records have been stored in physical paper file formats, which are difficult to access, maintain and share. To improve access health care records have to be maintained and shared electronically in an Electronic Health Records (EHR)/ Electronic Medical Records (EMR) System.

The main aim of this project is to design an application which will allow users to publish their health records. The scope of the user domain range from patients to doctors to insurance companies. The information published in the system will be usable by anyone else, at the discretion of the publisher. The information in the application will be stored in a database. The stored data will be analyzed and the results will be useful for other patients and doctors.

One of the aspects of the application will be maintaining Personal Health Records (PHR) and Electronic Health Records (EHR). Individual users will enter information into their own PHRs while doctors will enter data into the EHRs of their patients through Web interface as well as mobile application.

The second aspect of this project will be specifying a Personal Privacy Policy (PPP) on the health records of the user. Users will specify explicitly from whom his data should be protected. Users can specify when and for which reasons his data should be revealed to a third party.

The third aspect of this project will be implementing Privacy Policy Enforcement Protocol. Whenever a request by a EHR data consumer is made to EHR, the EHR owner will lookup the PPP to make sure the requester is allowed to access the requested data.

The fourth aspect of this project will be notifying the user whenever his data is being disclosed to a third party for analytics or mashups. The application will follow the privacy laws defined in the Health Insurance Portability and Accountability Act.

The fifth aspect of this project will be generating reports on users demand. Users can demand reports on weekly, monthly, yearly basis. Also, user can find all the reports online whenever he/she needs it.

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| 1 | Introduction | 5 |
| 2 | Literature Survey | 7 |
| 2.1 | Privacy Issues | 7 |
| 2.2 | Industry Trends | 8 |
| 3 | Privacy Laws | 10 |
| 4 | Proposed Approach | 13 |
| 4.1 | Personal Privacy Policy Module | 14 |
| 4.2 | Privacy Policy Enforcement Protocol | 16 |
| 4.3 | Disclosure Notification Module | 16 |
| 4.4 | Auditing and Monitoring the disclosure and Reports on demand Module | 17 |
| 4.5 | Implementation of Prototypes | 17 |
| 5 | Work Plan | 18 |
| 5.1 | Weekly Plan | 18 |
| 5.2 | List of Deliverables | 19 |
| 6 | References | 20 |

1. **INTRODUCTION**

Health care records form an essential part of a patient’s present and future health care. As a written collection of information about a patient’s health and treatment, they are used essentially for the present and continuing care of the patient. In addition, medical records are used in the management and planning of health care facilities and services, for medical research and the production of health care statistics. Doctors, nurses and other health care professionals write up medical/health records so that previous medical information is available when the patient returns to the health care facility. The medical/health record must therefore be available. This is the job of the medical record worker. If a medical record cannot be located, the patient may suffer because information, which could be vital for their continuing care, is not available. If the medical/health record cannot be produced when needed for patient care, the medical record system is not working properly and confidence in the overall work of the medical/health record service is affected [1].

Previously health care records were stored in physical files, which made availability and accessibility of health care records difficult. But now-a-days with technological advancement even the medical records need to be stored electronically. This gave birth to Electronic Health Records (EHR) and Personal Health Records (PHR). EHR and PHR are electronic records initiated and maintained by doctors and individual respectively. These records in digital format are capable of being shared across different health care settings, by being embedded in network-connected enterprise-wide information systems. Thus, by sharing this information on World Wide Web it will be easily available and accessible for doctors as well as patients anywhere in the world. It would be of great importance especially at the time of emergency and also for study and research purpose.

But, in this day and age not many people are comfortable about having their entire medical history recorded and digitized for almost just anybody to see – in other words, incursion into people’s privacy. The confidentiality of doctor - patient relationship is still sacrosanct. Besides, medical data can be used against a person in some cases – be it for a job application, insurance coverage or a college scholarship. Although it is against the law to discriminate against people with illnesses and disabilities, it is a fact of life that the fitter you are, the more competitive you are in the job market. The planned incorporation of genetic data in EMRs further adds to people’s fear of incursion into their private sphere [2].

Also, very few people are confident about the data protection and security of electronic data such as those stored in EMRs. Many people are not convinced that their data are safe from those who would want to misuse it [2].

In the project, we plan to provide a secure sharing environment of electronic health records and personal health records by proposing a personal privacy policy control system. This system allows the end users (patients) to specify their privacy policies that can be looked up and shared before the health records are being accessed and shared. We plan to develop a user friendly Web-based and mobile prototype system to create and update the access control policies for the private health records. In addition, we develop a disclosure notification system in case of the EHR or PHR to be shared with third party organizations or applications. We will develop the PPP data model and a protocol of looking up the PPP in case of the EHR or PHR access requests.

**2. LITERATURE SURVEY**

**2.1. Privacy Issues**

A major risk which concerns consumers relates to the privacy of health-related data. Most patients desire to keep their medical problems confidential, not only to eliminate embarrassment regarding the condition but also to protect against legal troubles. For instance, if a medical record was exposed and revealed that the patient has AIDS, the patient could face trouble acquiring health insurance or obtaining a new job. To address such risks, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule was enacted to protect the confidentiality of patient’s protected health information from improper use or disclosure (HHS OCR 2003). A supplement to HIPAA, known as the Security Rule, was implemented to assure the confidentiality of electronic protected health information by specifying a series of administrative, technical, and physical security procedures (HHS CMS 2007). However, laws cannot prevent the possibility of human errors or the persistence of hackers.

Another consumer privacy concern pertains to moving sensitive medical records from paper to a digital format, then placing those records on a system that can possibly be accessed from anywhere in the world. According to the Privacy Rights Clearinghouse (2005), over 218 million data records have been stolen since January of 2005 with at least 34 million of those records being medical information. The U.S. Department of Health and Human Services reports that approximately 150 people including nurses, clinicians, and billing clerks have access to at least part of a patient's medical record (Los Angeles Times, 2006). When including payers, providers and other entities that convert raw data into billing data, that number jumps up to approximately 600,000 people with access. And this is without the majority of hospitals using any type of health information management system for EHRs [3].

The only way to protect privacy is to give control over decisions for medical record sharing to individuals. Thus, those of us concerned with protecting medical privacy should not seek big-government solutions. Instead, we support the dissemination of personal health information, to be made by voluntary agreements between patients and those to whom they entrust their care.

**2.2. Industry trends**

EHR: A typical EHR has information about your health conditions, allergies, treatments, tests, and medications. Many EHRs can connect with health care providers outside your doctor’s office such as specialists, labs, imaging facilities (X-rays, CT Scans, MRIs), and the local hospital. This allows your doctor to share up-to-date information with your other providers as well as getting quick and easy access to your tests and hospital information.

Since everyone involved in your health care can share accurate information, your EHR can help lower the chances of medical errors and may help improve the quality of your health care. Some EHRs have warning systems built in to let your doctor know about drug allergies or potential problems with drug interactions.

Also, some EHRs have medical alerts to remind your doctor to perform certain tests or procedures. For example, if you have diabetes, your doctor’s EHR may remind your doctor to check your feet at every visit or order a blood sugar test.

PHR Networks: Microsoft launched Health Vault that promises benefits in healthcare information storage and sharing online but raises concerns on privacy of this information. Health Vault is Microsoft’s “new personal health platform that lets you gather, store, and share health information online.” Service users need a Windows Live ID to use the service. Once users create both a sufficiently safe username and a strong password, they can enter data from health and wellness devices, or upload documents to their vault. Users can then share this information with other Windows Live ID users, such as other patients or doctors.

Google also has a similar website entitled Google Health that is similar to Microsoft’s consumer oriented approach to health information. Both companies’ focus on this field is a result of current trends. In 2007, 52 percent of adults in the US searched the web for health information compared to 29 percent in 2001. More and more, patients are confronting their health care providers with information gathered from websites such as WebMD. Both Google and Microsoft hope to leverage their expertise in web search functionality with personal health information storage and sharing.

Microsoft’s Health Vault privacy statement addresses some privacy concerns while it does not specifically address HIPAA regulations. First, the privacy statement asserts that third parties, such as companies Microsoft hires to answer customer service questions, have access to personal information such as IP addresses and email addresses. However, Microsoft also states that these third party companies are required to maintain confidentiality. Second, Microsoft states that this information “may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or agents maintain facilities.” Third, the statement asserts that “aggregated information from the Service for marketing” may be disclosed. While, this aggregated information is not associated with any individual account, it may be used for marketing after an “opt-in consent” from the user. Finally, the privacy policy specifically addresses cookie use, web-beacon use, and encryption using HTTPS. While these assurances are definitely in the right direction, Microsoft will certainly want to assure compliance with HIPAA’s privacy and security rules.

Considering that Google’s use of cookies has been under the spotlight before, we are looking forward to review Google’s approach to both the privacy and security of personal health information [5].

**3. PRIVACY LAWS**

Privacy law is the area of law concerned with the protection and preservation of the privacy rights of individuals. Increasingly, governments and other public as well as private organizations collect vast amounts of personal information about individuals for a variety of purposes. The law of privacy regulates the type of information which may be collected and how this information may be used and stored [4].

The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information” (PHI)[[1]](#footnote-1) that is linked with 18 identifiers:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators(URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

“Individually identifiable health information” is information, including demographic data, that relates to:

* the individual’s past, present or future physical or mental health or condition,
* the provision of health care to the individual, or
* the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)

The Privacy Rule, a Federal law, gives you rights over your health information and sets rules and limits on who can look at and receive your health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule, a Federal law that protects health information in electronic form, requires entities covered by Health Insurance Portability and Accountability Act (HIPAA) to ensure that electronic protected health information is secure.

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g [6].

We call the entities that must follow the HIPAA regulations ***covered entities***.

Covered entities include:

* **Health Plans**, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
* **Most Health Care Providers**—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
* **Health Care Clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

**4. PROPOSED APPROACH**

Changing physical health records into Electronic Health Record (EHR) to improve sharing, availability and rapid transmission of medical information and making health care systems more efficient is need of time. Access control policies will be in hands of individual. Individual user will specify who will access his health records and when. Implementing in cloud environment will help other users, doctors, clinicians, insurance companies and third parties to look up health records of patients from anywhere in the world. Thus the main aim of health records availability will be satisfied, while the privacy wishes of the individuals are honored at the same time.

The overall architecture of the PPP control system is shown in Figure 1.

Patient

PPP (policies)

PPP Specifications

Web, Mobile devices

Disclosure Notification

PPP Query Processing

Monitoring & Auditing

PPP Lookup/Enforcement

3rd Party

Software

EHR

Aggregator

Doctors

**Figure 1: Architecture of PPP Control System**

**4.1. Personal Privacy Policy Specification Module**

We propose to develop a Personal Privacy Policy Module which allows users to share their EHR with their own personal settings. One of the major tool that module will consist of is privacy policy specification tool. With the help of privacy policy specification tool user can explicitly mention which data of his should be protected, who can access his data except him, when can his data be accessed-under what circumstances and condition. Also, user can specify what should be done with his data in case of emergency, even a user can ask for a notification whenever his data is been access by someone. See figure 2.

Another tool that module will have is privacy policy modification/update tool. With the help of this tool a user can modify or update or change his previous personal policy settings.

Personal Health Data

Whom to share with

USER

Doctor - General Physician

Doctor - Specialist

Reports

Some extra tools

Weekly

Monthly

Situation

Emergency

Yearly

Police

Insurance

Online Check

Some extra tools

**Figure 2: Personal Privacy Policy Specification Module**

The client tools for PPP specification will be developed with a Web interface as well as a mobile interface. This client tools will communicate with the server specification processing to interface with the policy database.

* 1. **Privacy Policy Enforcement Protocol**

We will model a privacy policy enforcement model. When a request by a EHR data consumer (covered entities, applications, 3rd party data processing programs, etc.) is made to EHR, the EHR owner (e.g. clinicians or hospitals) will look up the PPP to make sure the requester is allowed to access the requested data. The PPP owner (patient) need to register its PPP URI at the EHR data holder. The lookup utility communicates with the PPP to check the PPP policies before it releases the data. We plan to develop the details of this protocol in the project.

* 1. **Disclosure Notification Module**

Whenever a information will be disclosed to a third party for analysis or mashups, a user, whose information is being revealed should be notify. In personal privacy policy tool a user should specify that when and why he should be contact, if his data is being access. Patients should specify the notification parameters, example if patient’s physician access his data he won’t opt for notification but in other cases of data extraction patient may opt for notification. Also, a user may opt for regular notification alerts it can be weekly or monthly. In this way a user can be assured of his personal data usage. See figure 3.

Doctor

Notify Disclosure to Specific User & Deliver Reports

Electronic Health Records

Third Party

Any other User

**Figure 3: Disclosure Notification Module and Auditing, Monitoring & Reports on demand Module**

* 1. **Auditing and Monitoring the Disclosure and Reports on demand Module**

Each access of Electronic Health Record of any user will be closely monitored. And information to be disclosed will be according to the Personal Privacy Policy parameters set by the user. Reports generation module will generate report as and when needed by the user. The reports delivery can be weekly, monthly or yearly. Also, user can find all the reports online whenever he/she needs it.

* 1. **Implementation of Prototypes**

With the advent of cloud computing as a new computing paradigm, flexible services can be transparently provided to users or any other third party over the dynamic cloud environment where multiple users interact. By tapping into the cloud infrastructure, users can gain fast access to applications and drastically boost computing resources in a cost-effective way [8]. We plan to develop PPP control system and PPP database on a cloud. The client tools will be developed with Web interface as well as a mobile application that can interact with the server components on the cloud. For mobile applications we may use Android cell phones.

1. **WORK PLAN**
   1. **Weekly Plan**

|  |  |
| --- | --- |
| **Week** | **Proposed Weekly Plan** |
| **Week 1** | Design PPP repository Schema: ER Diagram. |
| **Week 2** | **Implementation of approved** PPP repository Schema **Design.** |
| **Week 3** | Design Personal Privacy Policy Module. |
| **Week 4** | **Implementation of** Personal Privacy Specification tool. |
| **Week 5** | **Implementation of Mobile** Personal Privacy Policy tools. |
| **Week 6** | **Testing of** Personal Privacy tools. |
| **Week 7** | Design Disclosure Notification Module. |
| **Week 8** | **Implementation of** Disclosure Notification Module. |
| **Week 9** | **Continuation of** Disclosure Notification Module. |
| **Week 10** | **Testing of** Disclosure Notification Module**.** |
| **Week 11** | Design Auditing and Monitoring the Disclosure and Reports Demand Module |
| **Week 12** | **Implementation of** Auditing and Monitoring the Disclosure and Reports Demand Module |
| **Week 13** | **Continuation of** Auditing and Monitoring the Disclosure and Reports Demand Module |
| **Week 14** | **Testing of** Auditing and Monitoring the Disclosure and Reports Demand Module |
| **Week 15** | **Integration of** Personal Privacy Policy Module, Disclosure Notification  Auditing and Monitoring the Disclosure and Reports Demand Module |
| **Week 16** | **Final testing of whole project** |

* 1. **List of Deliverables**

**a. Personal Privacy Policy Specification Module**

Input: Personal Privacy Policy data of users

Output: Entry in the PPP database

Interface: Web-based and Mobile App that people can download to their smart devices.

**b. Disclosure Notification Module**

Input: Health data by third party

Output: Notify specific user whose data has been extracted

**c. Auditing and Monitoring the Disclosure and Reports on demand Module**

Input: Data extraction by any one or reports demand by user

Output: Notify specific user whose data has been extracted, display generated reports to user

**d. Privacy Policy Enforcement Protocol**

**e. PPP Repository**

1. **References**
2. World Health Organization, Medical Records Manual: A Guide for developing countries.
3. Problems with EHR

<http://healthworldnet.com/HeadsOrTails/electronic-medical-records-the-pros-and-cons/?C=6238> , October 12, 2010.

1. Privacy issues

<http://www.thefreelibrary.com/Consumer+privacy+issues+associated+with+the+use+of+electronic+health...-a0219002331>, October 13, 2010.

1. Wikipedia

<http://en.wikipedia.org>, October 15, 2010.

1. Microsoft Health vault information

<http://blog.tsibouris.com/2007/12/microsoft-health-vault.html>, October 15, 2010.

1. HIPAA

<http://www.hhs.gov/ocr/privacy/hipaa>, October 14, 2010.

1. Janice Warner and Soon Ae Chun, Privacy Protection for Government Mashups, *Information Polity*: Volume 14, Editions 1 & 2, 2009: pp 75-90.
2. Hema Andal Jayprakash Narayan and Mehmat Hadi Guines, Ensuring Access Control in Cloud Provisioned Healthcare System, Department of Computer Science & Engineering, University of Nevada, Reno.

1. Wikipedia http://en.wikipedia.org/wiki/Protected\_Health\_Information [↑](#footnote-ref-1)