Study on Electronic Health Record
and its Implementation
Study on Electronic Health Record and its Implementation

Abstract:
This degree project deals with electronic health record (EHR). The report is divided into two main sections; literature study on electronic health record and an EHR system implementation. In the literature study section, EHR background, development history and service condition are introduced. The paper focuses on the sharing of medical information in different users, data safety and privacy. The adjunctions of computer science, technologies are used to solve the medical informatics’ problems. In the implementation section, based on the study of the current EHR systems, the design and implement of a shared EHR system are presented, which can be accessed by different doctors and patients. Access control function and cryptography protections are included in this system. The system test and evaluation are also given.
4.5.2 Patient Part ................................................................. 29
4.5.3 Doctor Part .................................................................. 31
4.6 Test and Evaluation .......................................................... 32
  4.6.1 Change on Record......................................................... 33
  4.6.2 Add new record ........................................................... 35
  4.6.3 Background Tests ......................................................... 36
  4.6.4 Black Box Testing ......................................................... 39

5. Result and Conclusion .............................................................. 41
  5.1 System Interoperability and Access Control ......................... 41
  5.2 Conclusion ..................................................................... 42

6. Recommendations for Future Work ........................................... 44

7. References ............................................................................ 45
  7.1 List of References ........................................................... 45
  7.2 Personal Contacts ............................................................ 46

8. Enclosures ............................................................................ 48
  8.1 List of Acronyms ............................................................ 48
  8.2 List of Full Papers ........................................................... 50
1. Introduction

1.1 Background

With the development of medical science, more and more information is needed for doctors to treat patients. Traditional handwriting health records had been insufficient to record so much information. The traditional paper records have two main inadequacies. The first is the misunderstanding caused by hand writing. At the end of 2009, the number of doctors for a thousand of urban persons in China is 1.75[1], which means every doctor should deal with about five hundred patients. This makes the doctor’s workload is very large. Doctors writing may become illegible and increase the possibility of mistake. The second inadequacy is that the paper records are difficult to save and search.

It was reported that between 44000 and 98000 deaths occur annually as a consequence of medical errors within American hospitals alone.[2] The medical negligence, unbalance in medical quality, the information sharing between doctors and patients limited the development of medical service. Among these, the biggest obstacle to improving the quality of medical service is how to realize the sharing of medical information which collected by different hospital or speciality health agencies. With the rapid development of medical technologies, the treatment process becomes more complex. The number of medical data and new acknowledges are in an explosive growth. Doctors need to record much more information. A health record system based on handwriting can not adapt to this rapid increasing. Furthermore, some of the medical information can be used by medicine companies to improve their products, or for government department to analyse communicable diseases. That information is usually not collected by hospital. They collected by different medical agencies. Those agencies are using different information systems, and also transmit and store the information in a different data structure. Therefore, interoperability between different hospital information systems has becomes a popular research area. The widely used of electronic health record system which has interoperability, decision support and remind function can significantly reduce medical accidents.

At the beginning of the study in Health Information Technology (HIT), the information system was used for medical transactions. After that the researches began to focus on Hospital Information System (HIS). HIS is used to manage the information flows created in the hospital. The Electronic Medical Records (EMR) took an important part in medical informatics. EMR is a basic model of electronic health records (EHR). The first EHRs were designed and deployed between the late 1960s and early 1970s.[3] EHR is a record that may include kinds of data. The data include personal information, medical history, allergies, laboratory results, medicine used history, immunization status, and even some sound and image (CT images) data. In1996, Waegemann proposed five levels in EHR development.[4]
First level: Automated Medical Record, AMR. 
Still based on paper record, but approximately 50% patients’ data are generated and saved by computer, and then print out the paper record.

Second level: Computerized Medical Record System, CMRS. 
Realize the same function as paper record in a digital scan method, it’s possible to visit older records. But users can not organize the data by their will, for example the data information can not form in an image.

Third level: Electronic Medical Records, EMR 
Has the same data range as the second level, but the data can be organized. The purpose of EMR is to realize the interoperability inside an institution. EMR has following features: Recognize all the patients’ information in one institution; provides patients’ information to all the medical service workers; provides a common work station for all kinds of applications and services.

Forth level: Electronic Patient Record System, EPRS 
More widely information is recorded in patients’ health record. It included one person’s all medical health related information, it’s not just limited in a specific scope of space and time.

Fifth level: The Electronic Health Record, EHR 
The broader terms of electronic medical records, provides health information not only used in medical agencies in traditional, also included life customs, self collection or clinical workers, parents, caregiver provided behavioural information.

Waegemann predicted the forth and fifth level will be realized in 2002. But until now, even in the most developed medical information technology countries are still not up to Waegemann’s prediction. These countries invested heavily in building available EHR. The United States American Recovery and Reinvestment Act (ARRA) of 2009 provides up to $34 billion for meaningful use of certified EHR systems.[5]

1.2 Aim and Purpose

The main purpose of our research is to study the current EHR systems, hoping to find out the limitation of the third level EHR, highlight why interoperability is so important to nowadays EHR systems. Several EHR systems are being evaluated. How those systems are used to solve the communication requirement of an interoperability system. There are some open sourced standards are used for the inter-system communication. Interoperability EHR system is a kind of distributed system, the same as other distributed systems, with the increase of communication, data security and privacy took a more and more important role in the system. Security and privacy are necessary measurements to measure an EHR system whether it’s reliable or not.
Access control is considered as an effective method to improve EHR system’s security and privacy. In the literature review part, five models about access control will be discussed.

Based on the knowledge from the literature review, design and implement an EHR system. The system can store the basic information of medical record, and share information between doctors and patients. In this system the patient has the right to control the access to their medical records. During the transmission, user’s information is encrypted by AES (Advanced Encryption Standard), to prevent information theft.

1.3 Methods and Resources

A systematic literature review focus on EHR system was taken. Three steps to search articles. (1) Databases Chosen. (2) Key words chosen. (3) Articles chosen. All the articles read and used in the review are from following databases: ACM, Cinahl and Medline. Articles’ abstracts were read and classified the articles into different classes. Excel sheets were created for statistics analysis. The requirements of EHR system were collected in Hospital of Guangxi Medical University. The EHR system implement in this study is based on the real condition provided by Hospital of Guangxi Medical University. The result of literature review will be used in the implementation of EHR system. The system test and evaluation will be conducted.

1.4 Acknowledgements

We acknowledge the help and support from our instructor Eric Chen and examiner Kamilla Klonowska; Doctor Huang Ping and doctor Li Kehui from Hospital of Guangxi Medical University; Experts Huang Shuhai from Guangxi CDC, and Engineer Li Bin from Guangxi Torch High Technology Development Company.
2. Literature Study

2.1 Literature Search

A systematic research is taken to generate meaningful result of our purpose. Three steps were taken to search and narrow the results: (1) A broad search using the most relevant key words for more potential hits. (2) More restrictions were used to filter the articles that were not related to the review. (3) Reading all the final results, eliminating some articles that not interested in this study, and classify all remained articles.

Medline and Cinahl databases were first selected to do this search. But in these two databases the articles which are related to EHR mostly are not related to computer science. Then ACM database was chosen to make this search. All the key words were divided into four categories: ‘Topic’, ‘Technology’, ‘Implement’, ‘develop’.

207 articles were found in the first step of search. All the articles were published from 2000 to 2012. It shows that in the recent ten years, researchers were interested in the integration and security of EHR systems.

ACM database
Key words are divided into four categories:
(3) Implement: ‘implement’, ‘implementation’, ‘design’, ‘research’

207 articles were found.
196 articles can find full text.
71 articles were using computer-based technologies.
25 articles meet the requirement of this study
11 articles discarded since no full text found
125 articles discarded since not mention about computer technologies
46 articles discarded since not met the computer based information sharing system

Figure 1. Articles Search Process

Key word ‘EHR OR electronic health record’ is used in ACM database. As a result,
207 articles were found in the search. Some restricted conditions were used to narrow down the results: (1) Full text was necessary. (2) EHR system should be the topic because some articles just mention EHR and has no detail. (3) Computer-based technologies were used to solve the EHR interoperability problems. (4) Using computer as platform, not mobile or other devices. (5) Information sharing or safety was mentioned. Conference articles were not included in the final result.

After the first time of search, 11 articles which had no full text were eliminated, 196 articles remained, which means 94.69% articles had full text in this search. All the 196 articles’ abstracts and contents were read, 125 articles were eliminated, those articles mentioned neither EHR as a system, nor computer technologies to address the EHR problems. Some of the articles were excluded because of non computer platform, the communication between medical devices’ sensors or mobile platform based systems were not included in this study. Two main reasons were put to use: (1) Lack of computer technologies involved. (2) Discussing EHR in a management way, but not in a system design way.

The remained 71 articles of full text were read, 25 of them met the requirement of computer-based information sharing EHR system, and the main area of data security and privacy: access control. Three sheets were created to classify the result of each step of search.


Sheet 2 contained 10 articles, all the articles were focused on information sharing. The creation of Sheet 2 was based on the result of Sheet 1 class ‘Sharing’. The articles were classified into: ‘No.’, ‘Title’, ‘Purpose’, ‘Technologies’ and ‘Problem solved’ five classes.

Sheet 3 contained 16 articles. Those articles focused on access control in information sharing EHR system. Sheet 3 was also based on the result of Sheet 1, from class ‘Access control’. The articles in this sheet were classified as the same way as Sheet 2.

2.2 Articles Statistics

A statistics consequence was taken based on the 207 articles. As classified method mentioned above, all the articles were from ACM database, they were numbered from No.1 to No.207, according to relevance of articles.

The majority of articles are from USA, 96 articles take 46.37% of total. From the result, almost half of the EHR research works were done by USA throughout the
entire world. USA has the largest number of researchers, the most financial aid and the most advanced computer technology. That led to its most advanced EHR system. As other information systems, USA’s researches in EHR system are leading the world.

The second is Europe. 52 articles were done by European countries, included UK (16), Denmark (10), Germany (5), Sweden (4), Spain (4), France (3), Italy (3) and Norway(3). 52 articles account for 25.12% of total. In Europe, UK makes the most effort in EHR researches. Nordic countries (Denmark, Sweden and Norway) have totally 17 articles, which reflect North Europe countries also attach importance to EHR. Their achievement may benefit from the development of their computer technologies.

The third is Canada. 21 articles are from Canada, take 10.14% of total. There is a very famous institution in Canada called Canada Info Way, with an aim to provide a free development platform to improve E-health, which encourage technicians to make researches in EHR.

In Asia. 10 articles were found (4.83%), Korea (7), China (2) and Japan (1) were included. Although China is still in a phase of changing paper records to electronic records, the government still realizes the importance to build up a national interoperable EHR system. Korea and Japan have the most advanced technologies in Asia. Japan is one of the earliest countries to develop EHR.

Most of the articles were issued as ‘proceeding’, 170 articles (82.13%) were ‘proceeding’. The rest of the articles were issued as magazines (6.76%), journals (6.28%), newsletters (3.38%) and conferences (1.45%). All the articles were published from 2000 to 2012.

<table>
<thead>
<tr>
<th>Year</th>
<th>Articles</th>
<th>Percentages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>34</td>
<td>16.43%</td>
</tr>
<tr>
<td>2011</td>
<td>56</td>
<td>27.05%</td>
</tr>
<tr>
<td>2010</td>
<td>40</td>
<td>19.32%</td>
</tr>
<tr>
<td>2009</td>
<td>24</td>
<td>11.59%</td>
</tr>
<tr>
<td>2008</td>
<td>18</td>
<td>8.70%</td>
</tr>
<tr>
<td>2007</td>
<td>10</td>
<td>4.83%</td>
</tr>
<tr>
<td>2006</td>
<td>9</td>
<td>4.35%</td>
</tr>
<tr>
<td>2005</td>
<td>5</td>
<td>2.42%</td>
</tr>
<tr>
<td>2000-2004</td>
<td>11</td>
<td>5.31%</td>
</tr>
</tbody>
</table>

As shown in Table 1. From 2000 to 2004, the number of articles from was similar each year. From the year 2005, the number of articles begins to increase. It increases every single year after 2005. Only in the first five month of 2012, 34 articles were issued, more than half of the articles from 2011. This growth reveals the study of EHR.
is becoming a trend. People now more and more realize the importance of a usable EHR system. More and more institutions are interested in it. ACM database is a database which aims at computer technologies. The result of this statistics analysis also shows the integration of computer science and medical science. Computer is thought of as an effective tool to solve problems existing in medical field.

2.3 Purpose Classified

All the articles were classified into eight groups. These eight groups cover all the articles. There were just four groups at first: ‘Sharing’, ‘Security’, ‘Standard’, ‘Design’. Along with the read went deep into, the ‘Security’ separated into ‘Access control’, ‘Cryptography’, ‘Security & Privacy’. The ‘Design’ was divided into ‘Design & Implementation’ and ‘Analyse’. The safety topic was divided into ‘Access control’, ‘Cryptography’ and ‘Security & Privacy’ three different classes due to their speciality. Articles in ‘Access control’ class focus on the access control models. Articles in ‘Cryptography’ class focus on the data encryption and decryption during the transmission. ‘Security & Privacy’ is a comprehensive class, there is some security or privacy functions just mentioned in few article, so they were all put together into one class.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Articles</th>
<th>Percentages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing</td>
<td>67</td>
<td>32.37%</td>
</tr>
<tr>
<td>Access control</td>
<td>46</td>
<td>22.22%</td>
</tr>
<tr>
<td>Cryptography</td>
<td>12</td>
<td>5.80%</td>
</tr>
<tr>
<td>Security &amp; Privacy</td>
<td>50</td>
<td>24.15%</td>
</tr>
<tr>
<td>Standard</td>
<td>26</td>
<td>12.56%</td>
</tr>
<tr>
<td>Web Service</td>
<td>51</td>
<td>24.64%</td>
</tr>
<tr>
<td>Design &amp; Implementation</td>
<td>52</td>
<td>25.12%</td>
</tr>
<tr>
<td>Analyse</td>
<td>71</td>
<td>34.30%</td>
</tr>
</tbody>
</table>

Table 2. Articles in Different Purposes

Only abstracts and contents of these articles were read. The classification was mainly based on the abstracts and contents of the articles. The key words were also taken into account. First six groups were used to distinct the main purpose of the articles. The last two groups were aimed at defining whether the article was about a new system design and implementation, or an analysis at existing system.

2.4 Interoperability of EHR.

The International Standards Association (ISA) defined that the EHR should be a repository of information regarding the health care in a computer readable format. It can be accessed by multiple users in a safe way. All the users have their own authority, medical records can be accessed when and only when visitor had been authorized. Its primary purpose is to support continuing, efficient and qualitative integrated health care [6].
Imagined a few scenarios: (1) A patient takes a medical treatment at one hospital, but he may concern to multiple medical laboratories. Most of his diagnosis material in different laboratories may be duplicated. (2) A patient in his whole life may not only go to one hospital, when he goes to a new hospital, the physician may use his diagnosis material from other hospitals. When he needs multiple health cares from different places for one treatment, those places may spread cross the whole country. (3) When a patient who has serious drug allergies, which is important for doctors to know his allergy history.

A patient is likely to receive medical attention from several hospitals over his lifetime, so it is reasonable for each hospital to have unrestricted access at any time to the previously recorded patient's data [7]. The interoperability of EHR system can bring solution to those problems. With an integrated EHR system, all the different laboratories can quickly deliver and share the patient diagnosis not only inside one hospital, but also between hospitals. That may reduce the duplication of physical examinations, reduce the cost and resources using in the medical field. China particularly, it now faces a shortage of medical workers, which causes serious conflicts between doctors and patients. An interoperability EHR system may satisfy the requirement of more medical workers. Sharing vital information like histories of adverse drug reaction can decrease deaths and other serious consequences [7]. The genomics data included in the patients’ record can help improve health knowledge, strengthen diseases prevention, diagnosis and treatment.

The state of electronic information integration in Health Care lacks far behind other business domain such as banking, insurance, and electronic commerce [8]. The realization of this fact and the ongoing cost explosion in the Health Care sector has caused a surge of companies and public organizations trying to develop EHR systems to meet this need [8]. The reason of this lack may be the complex policies in medical field. Patients’ medical records are very sensitive. Privacy is the most important quality in an information system. Lots of policies are announced to protect the privacy of medical records. When design an EHR system, all the policies should be take into account, which results in the difficulties in design such a system. Medical science is improved rapidly in recent decade. It requires more space to store medical information. A safe, reliable and information sharing system is necessary. With the encouragement of each country’s medical department, companies and public organizations now show great interests in develop EHR system.

It should be noted that the interoperability of IT systems can be assessed on different levels, from the communication protocol and service level to the behaviour of the system as perceived by the end users [10]. Interoperability defined by HL7 has three parts: Technical, Semantic and Process [11].

Technical part: Technical interoperability focused on the health data transmission and the security during the communication. Both sides of the transmission form the data in
a standard format.

Semantic part: The interoperability based on the relevance between both communications participants of their transmitted information. A semantic tool was used to interpret from one participant to another.

Process part: Process interoperability concentrates on higher-order workflow that makes the shared data experience valuable [12].

Table 3. Articles Focused on Interoperability Analyse (1)

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Towards electronic health record support for collaborative processes</td>
<td>Realize information interoperability and cooperation based on openEHR.</td>
</tr>
<tr>
<td>10</td>
<td>Patient-centric authorization framework for sharing electronic health records</td>
<td>System work in a middle ware form, integrate decentralized patient information.</td>
</tr>
<tr>
<td>22</td>
<td>Semantic interoperability of clinical data</td>
<td>The role of semantic interoperability was used.</td>
</tr>
<tr>
<td>26</td>
<td>Achieving interoperability among healthcare standards: building semantic mappings at models level</td>
<td>Analyse how semantic mapping worked in model level.</td>
</tr>
<tr>
<td>49</td>
<td>A flexible approach for electronic medical records exchange</td>
<td>Evaluation in different standards, showing how to partially exchange.</td>
</tr>
<tr>
<td>52</td>
<td>A survey and analysis of Electronic Healthcare Record standards</td>
<td>Discuss kinds of information exchange standards.</td>
</tr>
<tr>
<td>63</td>
<td>Coordinating e-health systems with TuCSoN semantic tuple centres</td>
<td>Using TuCSoN to address semantic interoperability.</td>
</tr>
<tr>
<td>72</td>
<td>Service and model-driven dynamic integration of health data</td>
<td>Semantic interoperability.</td>
</tr>
<tr>
<td>74</td>
<td>Can GRID services provide answers to the challenges of national health information sharing</td>
<td>From multiple domains to analyse interoperability</td>
</tr>
<tr>
<td>145</td>
<td>Healthcare interoperability through enterprise architecture</td>
<td>Realized interoperability based on enterprise architecture.</td>
</tr>
</tbody>
</table>

Among those 10 articles, 4 of them focus on standards (40%) and 4 articles focused on semantic models (40%), another 2 articles (20%) about middleware technologies. Defined by HL7, standards are related to technical part of interoperability. Semantic models belong to semantic part, and the middleware technologies can be classified into process part.

Table 4. Articles Focused on Interoperability Analyse (2)

<table>
<thead>
<tr>
<th>No.</th>
<th>Technology</th>
<th>Problem solved</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>openEHR</td>
<td>Based on openEHR architecture to</td>
</tr>
</tbody>
</table>
support collaborative care delivery.

| 10 | openEHR, HL7 CDA, HL7 v3, XML-based HL7 CDA | Standards for share information, and access control. |
| 22 | openEHR, HL7 CDA, CEN-13606, The Reference Information Model (RIM) | Prevent patient from death by drug reaction; Prevent duplicated tests; Reduced the cost in chronic diseases. |
| 26 | Ontology Matching | Communication between existing heterogeneous systems. |
| 49 | HL7, DICOM, VMR, CVM, XML | Partially shared information, address the flexible problem. |
| 52 | HL7 CDA, CEN-13606 EHRcom, openEHR, Cross-Enterprise Document Sharing (XDS), ebXML | Discussed EHR standards, comparison and evaluation |
| 63 | TuCSoN | Combination of semantic support and middleware technologies |
| 72 | ePCRN | Large scale distributed system’s semantic interoperability |
| 74 | WSDL, UDDI, SOAP, XML, CORBA, Grid, HL7 RIM | Using multiple domains technologies addressed interoperability |
| 145 | Enterprise Architecture | The interoperability between EA systems. |

As Table 4 shows, in most of the articles, Standards take an important role in EHR interoperability. Several standards are under development to solve the interoperability problem: Health Level Seven (HL7); Digital Imaging and Communications in Medicine (DICOM); openEHR; CEN EN 13606 EHRcom (European Standardization Committee: Technical Committee for Healthcare); Integrating the Healthcare Enterprise (IHE).

The Health Level Seven (HL7) is a non-profitable organization. Its aim is to develop international health information interoperability standards. Several standards are used to form a stable format in data storage, and define models for exchange medical data. Clinical Document Architecture (CDA), an architecture used for clinical document. Stable data storage format and data exchange model is defined in this architecture. Hospitals using this architecture can form clinical document in the same organization, this provides the foundation for information exchange. HL7 v3 Messaging is the HL7 version 3 messaging standard which defines a series of electronic messages (called interactions) to support all healthcare workflows. HL7 v3 messages are based on an XML encoding syntax [13]. In a word, HL7 v3 Messaging define a message delivery standard. Message packaged by HL7 v3 Messaging from one EHR system which designed based on HL7 standard can read by another HL7 based EHR system.

The Digital Imaging and Communication in Medicine (DICOM) is a standard for handling, storing, printing, and transmitting medical images. It includes a file format
definition and a network communication protocol [13]. It is well known as its medical images sharing. This standard formulates the data storage and the massage delivery. DICOM uses TCP/IP as its communication protocol, while TCP/IP provides data format in end-to-end communication.

The CEN EN 13606 (European Standardization Committee: Technical Committee for Healthcare) Request and Report Messages for Diagnostic Service Departments document specifies a semantic data model and model-based compositional rules for messages, but only partial guidelines for electronic document interchange [14].

There are two main purposes for using standards: (1) Formulate the data storage organization. All the medical information can be arranged in a unify manner. (2) Medical information was formed in order and packaged under the rules of standards. The message receiver can analyse correctly following the same standard.

Standards are belonging to technical part of interoperability. Such standards can be used when a new EHR system is designed. Because of the lack of foundation and technicians in medical informatics domain, some big hospitals and medical institutions develop their own EHR system individually. That leads to the appearance of numerous heterogeneous systems. The integration of those heterogeneous systems is difficult, because those systems have already been designed and came into service. Previous patient data is stored in such systems, to move this data to a new system is not easy. The hospitals and medical institutions may not invest a new EHR system because such a system is expensive. The system interoperability also has some other difficulties: (1) Clinical information delivery may involve wide range of distributed health centre. It's a challenge to form a large scale of distributed system. (2) The standards development and deployed is in a slow pace. (3) Wide variation of patients’ privacy protected data control policies. So another kind of interoperability, semantic interoperability is taken into account.

In general, semantic interoperability is defined as the ability to receive some information and interpret it in the same sense as intended by the sender system, without prior agreement on the nature of the exchanged data [7]. For example, one hospital is designed in HL7 standard, the hospital has to communicate with other hospitals which are design in openEHR standard. Because they used different format in creating medical record, HL7 system can not read the massage send by openEHR system. In order to achieve semantic interoperability in a heterogeneous environment, the meaning of the information that is interrogated (or communicated) has to have the same semantics or meaning across the systems [15]. The purpose of semantic tools are to convert different presentation from different systems into a standard presentation, when the both sides of communication present the same meaning, semantic tools should recognize automatically.

The main advantage of semantic interoperability is that it can be used to communicate
with unknown systems. It’s not like the standardized systems. The standardized systems have already made agreement on the data storage and transmission format. When designing a new system, using existing standard is a good choice. When communicating with an unknown system, how to organize the information to fit that system? Even if the information format is known, a HL7 system can not generate an openEHR format record. There is an important concept called Ontology Matching, which is the process of eliminating the terminological and conceptual incompatibilities and discovering similarities between two ontologies. Semantic interoperability generally realizes a mapping way. For example, one system using phrase ‘blood type’ to present the type of blood, but another system using ‘blood group’. Therefore, a semantic tool forms a map from ‘blood type’ to ‘blood group’. All the words and phrases used in medical records from one system can map to another system’s words and phrases, so that a semantic map which records this correspondence is build.

Middleware technologies have the same purpose with semantic interoperability. Middleware technologies (e.g. CORBA) aim at communicating with heterogeneous systems which using different compile languages. Middleware can be explained as a translator. For example if someone knows different languages, he can interpret between people who using different languages. Middleware act like this people that knows many different languages. Middleware translate between systems that using different languages. Middleware integrates in a lower level than semantic integration. As the increase in decentralized computing scale, middleware, an essential mechanism for connecting and integrating distributed component systems, is becoming one of the central issues in industry and research [9].

GRID can be an answer to the medical information sharing. GRID is an integration of technical and semantic interoperability. Using HL7 Reference Information Model (RIM) as a semantic model, it can represent for the information carrying by the HL7 message explicitly. XML is used as a message transmission standard, Web used as information mediation and integrated service platform in GRID. Web service standards such as WSDL, UDDI and SOAP allow cross platform integration of different types of middleware networks using commonly available protocols and standards such as http and XML [9]. Middleware is used to connect different types of distributed system. In this GRID model, data store and transmit are under the order of standards. They can be mapped to other standards by semantic model. Web storage can help to create a decentralized system. This system can communicate and integrate by XML which is a common used technology in delivering message on the internet. This model can solve two main parts of interoperability at the same time: technical interoperability and semantic interoperability.

From the analysis above, a conclusion can be reached simply that: It will be better if a new system is design followed the standards such as HL7 and openEHR. In the integration of existed systems, most of the countries, semantic tools are now the best
way to address information sharing through using different EHR systems. But there is a limitation of semantic tools, the accuracy of ontology mapping. The medical field needs completely correct information, so the accuracy in using medical words is very important. The accuracy of the ontology map will affects the performance of the interoperability.

2.5 EHR Access Control

Interoperability of EHR system allows people store large amount of information in different place. In much of the developed world, healthcare has evolved to a point where patients can have many different providers– including primary care physicians, specialists, therapists, and even alternative medicine practitioners – to service their diverse medical needs [17]. There comes a big problem. The information sharing increases the risk of medical misuse and data theft. A medical record includes patients’ personal information, like telephone number and security number, which are private. Sometimes patients don’t want to share their diagnosis because it is not related to the diseases that they are treated. They just want to share the relative information to the physicians. Data theft can invade to patients’ medical records and stole patients’ records to do financial fraud. In order to prevent this crime, how to manage the access correctly becomes a key issue.

Health Insurance Portability and Accountability Act (HIPAA) places legal requirements on accessing control in systems that store patient data [18]. (HIPAA) Security Rule states that one must implement, “mechanisms that record and examine activity in information systems that contain or use electronic protected health information” [19]. Some access control models are underdevelopment to meet this legal requirement: Role-Based Access Control (RBAC), Digital Right Management (DRM), Usage Control (UCON), Tees Confidential Model (TCM) and Mandatory Access Control (MAC).

RBAC: A prospect succedaneum of traditional access control (Autonomic Access Control, Mandatory Access Control). In this model, the authorities are related to roles. When a user registers an EHR system, a suitable role will be assigned to the user. Users can have the authority of that role when they become a member of it. In an organization, roles are created to accomplish all kinds of works. Users are assigned to corresponding role based on their responsibility and qualification. Users can change their role, when their responsibility and qualification is changed. Generally, user’s authority depends on their role.

DRM: Pair of keys was generated, including public key and private key. The key pair is distributed by a third part called digital authorization centre which is trusted by users. Public key is used to encryption which private key is used to decryption. The message can be read only by the private key holder. The key pair is generated by the record creator. Benefits from using DRM:(a) Data in DRM systems is always in
encrypted form and thus inaccessible to unauthorized users (b) Users can only access to the data according to the policy stated in the license accompanying the encrypted data, and (c) DRM is contrary to traditional access control mechanisms, it can enforce the usage policy even when data is on a receiver’s terminal, thus, preventing unauthorized copying or distribution of data that may lead to authorized access [20].

UCON: Three elements: subject, object and right. Also another three elements are related to authorize: authorization rule, condition and obligation. The authority is based on the attributions of subject and object, and authority requirement. Access right can be assigned before or being the access actions. Mutable attribute is the most different quality compared with other access control models. Mutable attribute can change along with the change of access result. UCON model includes RBAC, MAC and DRM. It’s a new generation of accessing to control model.

TCM: In the TCM, permissions are additionally assign to users (called identities) irrespective of role, and introduce algorithms to process the several types of permission; also negative permissions, which deny access to resources that are used [21]. Users not only has role as RBAC, but they also has identity in this model. The identity is a branch of role. It defines more detail than role. It’s more individually because the identities can be assigned to each user. With identity, users can manage the right of access more flexible.

MAC: A mandatory control independent of user’s behaviour. MAC is managed by security administrators, instead of users. In MAC model, subjects (data) and objects (users) are classified into different security levels. To determine whether to grant or to deny users access is based on the comparison of the subjects and objects security level. For example, a chief nurse can manage all the patients she takes responsible to. A higher security level should be assigned by administrator before the nurse’s management. With higher security level she can access to the patients’ data which are in a lower security level.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Enhancing accountability of electronic health record usage via patient-centric monitoring</td>
<td>NHIN Direct, MAC</td>
</tr>
<tr>
<td>8</td>
<td>Privacy preserving EHR system using attribute-based infrastructure</td>
<td>ABE, Cloud, Patient-centric</td>
</tr>
<tr>
<td>10</td>
<td>Patient-centric authorization framework for sharing electronic health records</td>
<td>Patient-centric, RBAC</td>
</tr>
<tr>
<td>11</td>
<td>Flexible patient-controlled security for electronic health records</td>
<td>Smart card</td>
</tr>
<tr>
<td>16</td>
<td>Explaining accesses to electronic health records</td>
<td>User-centric Auditing</td>
</tr>
<tr>
<td>41</td>
<td>A purpose-based privacy-aware system using privacy data graph</td>
<td>RBAC</td>
</tr>
</tbody>
</table>
As Table 5 shows, 16 articles focus on access control and 10 of them use kinds of access control models (62.5%). The other articles are about access auditing (8, 10, 16, 71) and physically access control (11, 42, 64). In the access auditing mechanism, an access log will be created when someone accessed to the patient’s record. This access log can provide certification during the treatment because the access log can be checked. Everyone who had accessed the patients’ data, their name and purpose can be known during the patients’ treatment. Access auditing mechanism now focuses on the automatic creation of access log. Physically access control, physical material is used to store patients’ record. For example smart card, which similar to credit card. The card is embedded by an electronic chip. The chip is regarded as data storage. User’s personal information and medical records store in this chip. The smart card is held by user, it is user’s right to decide whether to share it or not.

Compared with all the access control models, UCON is a potential model for future design. It’s a new generation of access control model. A UCON based system is more complex than the others. It costs more money, spend more time to design and implement such a system. RBAC model is much easier to design than UCON model. It has efficient security and flexibility in EHR system. For an E-Healthcare organization, the Role-Based Access Control (RBAC) security model was found to be suitable because permissions are assigned to roles [22]. All the people in the hospital can be simply classified into two roles: patients and doctors.
2.6 EHR in China

In China, there is still a long way for EHR to be developed comprehensively. The main reasons are: (1) The development of electronic records at the hospital level just starts. (2) Such HIS, CIS, LIS, PACS systems that can provide information to EHR is not complete. EHR system’s information is based on the collection of those basic information systems. (3) So far has not established an inter-agency, cross regional management of the medical units of the electronic health record system [23].

In China, it just starts to develop EHR. The most important thing for developing EHR is to change paper records into electronic one. Although it just starts, it now develops fast. Because it’s different from USA and Europe, the informatics of hospital already developed for a long time. Lots of heterogeneous EHR systems have existed before a unify standard was published. Numerous different architectures and standards make it difficult to integrate those systems. In China, the most advanced technologies and theories from all over the world can be used to implement an interoperable EHR system. In other words, China can build up interoperable EHR systems from the beginning of the system’s design. Since there were not many EHR systems are being used, the interoperability problem of EHR systems in China can be solved.

To build an interoperable system, a unify standard is important. Chinese Ministry of Health has already published series of requirements for hospital informatics. A unify system architecture was defined. Since the HL7 has already existed and is commonly used all over the world, China set up standards based on HL7. All the new EHR systems can follow this international standard, which is useful for sharing medical records both nationally and internationally.

Similarly, the lack of foundation and medical informatics expertises in other countries also make troubles in their development of EHR. A simple formwork using standard such as HL7 or openEHR and fixed system architecture can be a reference to the future system design. Different hospitals can build up their own suitable system based on this formwork. Lots of duplicated works can be avoided.
3. User Requirement and Analysis

A research was taken in the Hospital of Guangxi Medical University. This hospital was found that some departments of it were already achieved medical informatics. Such as, patient information and medical records can store in the hospital’s information system in electronic form. In the survey had taken in the endocrinology department. In this department, the information process in this way, patients only allow to have paper records. Because of that in the process of diagnosis and treatment the records for the patients are handwritten by doctors. These paper records are just for the patients. On the doctors’ side, the doctor will type in the records into the hospital’s information system, and store the data in electronic way, which only can be visited inside the system.

However, such a system there is three serious drawbacks. (1) Patients don’t have records stored in electronic form, it makes the patient very inconvenient to save and view the records. Every time the patients want to visit a doctor had to bring their paper medical records. While doctors can found the records in the hospital system, they still need a hand-written copy for the patient. Although hospitals do not save a lot of paper medical records and it is convenient for the doctors to search the records. But all records require the doctors to write twice, one handwritten for patient, and one electronic version input to the system. So the hospital information system actually increased the doctor’s workload. (2) Due to the patient’s medical records are written in paper, when he needs to change a hospital, only paper records can be shown to the new doctor. Such sharing of information is very slow, and the handwriting may lead to misunderstandings. That can lead to very serious consequences. (3) The electronic medical records are stored in the system that created them. They can be shared only within the hospital. Even patients, the owner of their records, can not visit the electronic records. Don't even to control the access authority.

3.1 Patient’s requirements

Patients need a system that they can view their own electronic health record. Patients need to check their medical records in different hospitals in their own account. They hope they can manage the access authority. Patients need to have the right to assign the authorities. Patients can decide whether to allow doctors to access their personal information and medical record or not. They hope to add or delete the visitor’s permission in its own account. When a patient wants a doctor to check his information, he can login his account, grant the doctor the authority to access his medical records. When patients do not want the doctor to access his medical records, he can cancel the doctor’s authority. In this system, the patient can view their records whenever they want. When he needs to change a hospital, he can give doctors the permission to access their electronic health records. A good EHR system should be based on user-centred. Search function is needed in this system, patients can find the medical record they want using search function.
3.2 Doctor’s requirements

For the doctors, they would like a system that allows them to access the records from other hospitals’ information systems when they were authorized by their patients. So they don’t have to view a handwritten record. That can significantly reduce the medical accident caused by misunderstanding. Doctors hope they can not only read the patient’s medical record, but also can create new medical records and change the old medical records.

3.3 Administrator’s requirements

The system needs to be managed by administrator. In this part, there is a name list of hospitals. Hospitals in this list are allowed to share information with other member hospitals. Administrator need to be able to modify this list, add or delete hospitals in this list. Hospital wants to join the system need to apply to the administrator and then added by the administrator. All user accounts should be managed by the administrator. When doctors need to modify the patient’s medical records, sent application to the administrator, then administrator can decide whether agree with the doctor’s request or not.

3.4 Security requirements

To avoid abusive registration, all the users in this system can register only one account for each person. They had to use their ID number to register their account. In the registration, users can set up their password. Only the person who knows the password can login the account. The password is encrypted during the transmission. In the transmission of medical records and personal information, those information are encrypted. Even if the information is intercepted, the information theft can not read the information without the key.
4. Design and Implementation

In this chapter, based on the discussion given above, the design and implementation of a simple EHR system will be discussed. Compare those standards and models that used to solve the problems mentioned above. Choose a suitable solution. The results of literature review part will be considered in the implementation part of this study. Tools and models used to implement will be introduced before the implementation section. In the system functions section, the functions of the EHR system we designed will be presented.

4.1 Selection of Solutions

As mentioned before, lots of standard and access control models are used and developed. The EHR system implement in this study is based on the study of current standards and access control models.

4.1.1 Interoperability

There are two main solutions of interoperability now in use. The first is standard. HL7 and openEHR are the most popular standards. They have the same purpose. They aim at creating a world wide standard for the storage and transformation of medical records.

HL7 has developed for many years. The standards have been improved for many times based on a large scale of researches in the hospitals. It also includes the policies published by the government medical agencies. That makes HL7 become a very complex unit of standards. It’s hard to implement a EHR system fully based on HL7 standards. Multifarious of policies make it almost can not program. So, lots of the EHR systems do not fully use the standards of HL7.

The same problem happens in openEHR. Standards are too complex and involve too many policies, which makes such EHR system very difficult to realize. Lack of talent and foundation, various countries and industries have paid attention to the development of EHR. The development is still slow during these years. A variety of standards exist, and they have their share of the market, which makes the information sharing among different standards become a problem.

The second is semantic tools. The use and development of semantic tools are based on the development of Semantic Web. Semantic tools present a very suitable method of information sharing between heterogeneous systems, which make different medical institutions develop their own EHR system without sharing information with each other. But semantic tools are determined by on its accuracy. When the number of heterogeneous systems that need to interconnect with each other is not large, semantic mapping is easy to implement. However, if the number is large, it will make the semantic mapping complex. At the same time, it will reduce its accuracy. In the health
care system, if the semantic mapping is not accurate, it will lead to serious consequences. Therefore, the semantic mapping must be assured at a high level of accuracy. Such complete, accurate and efficient semantic mapping tool is difficult to implement.

These two information sharing solutions share one common feature, they are based on Client/Server architecture. User’s information need to be transferred between systems, both sides of the communication will inevitably need to achieve a communication standard. This had result in the problem mentioned before. However, in this study we will try to use Browser/Server architecture to solve this problem. In the B/S architecture, browser used as a user interface, Users can directly operate the database where the data being used is stored. User’s information transfer from one system to another is not needed. This can also guarantee the security of data in the database.

4.1.2 Access Control
In previous studies, several access control models are mentioned. These models essentially cover a wide range of access control methods. Among those models, UCON is the most flexible model. It includes two layers: a lower level for general authorization, and a higher level for individual authorization. But individual authorization is not very necessary in hospital information system. If a doctor needs a specific patient’s record, it’s not necessary for him to send application of individual authorization. He can just ask his patient to allow him to access the record. So compare with those models, we decide to use RBAC model. RBAC is very suitable for hospital information systems. Access control classification in RBAC is enough for hospital information system. In the hospital, doctors and patients are the main users. In RBAC model, doctors and patients can be divided into two roles. When the user registers, roles have to be selected (doctors or patients). Their authority will be allocated based on their role selected in the registration. From the programming, the RBAC model is relatively easy to design. This distribution of authority is an appropriate way for people to understand.

4.2 System Design
This system is designed based on the previously selected software architecture and access control model. First of all, it begins with the system architecture design. The two main functions information sharing and user access control will be realized based on this architecture. The system architecture is designed into two main parts called foreground and background. The foreground is for patients and doctors from hospitals. The background is operated by the system administrator.

4.2.1 Foreground
In this part of the system, patients can search, update and delete their personal information and medical record. But they can not change the medical records. The
doctors from hospitals can search, add patients’ medical record if the patients authorize to them, but they can not change or delete patients’ medical record. If they want to, they must ask Hygiene Department (administrator). If administrator gives the authority to them, they can change or delete the residents’ medical record. In this system, each user has their loginID and password. User’s loginID is fixed once they register in the system. But they can change the password by themselves. (Administrator registers all users) The foreground structure of this system is showed as Figure 2 below. Figure 2 shows the structure of the system foreground.

![Figure 2. Foreground Structure](image)

**4.2.2 Background**

In the background part, the administrator can increase or decrease the number of the users. It can also authorize to the hospitals so they can update the patients’ medical records. Then it can create or delete patients’ files also, it can mange the content of all files.

![Figure 3. Background Structure](image)
4.2.3 Interoperability
There are three databases. The first one is for patients include patients’ personal information, ex: name, age, address and so on. The other two databases simulate two different hospitals. One is for hospital A. It includes some patients’ medical treatment and their own information. The other one is similar, but it simulates another hospital called hospital B. This is a sample system, so just two hospitals are simulated in this system. If more hospitals passion to use this system, they can just easily add their databases into this system.

Information sharing is realized in this way. Different hospitals have their own database. For example, a patient has a surgery in hospital. His medical record is stored in A hospital's database. When he goes to hospital B, the doctor from hospital B need to check the record created in hospital A. The doctor can ask the patient to change the access authority. If the patient agrees, he can login his account and authorize the doctor from B hospital to use the record from hospital A.

4.2.4 Access Control
(1) Patients: In registration, if the user is a patient, will be assigned to the patient role. In a patient role users can only access their own medical records and can not access to other patients’ medical records. Patients will never be authorized to access other patients’ records. Patients can not add, delete their medical records, because the medical records should given by the doctors, not the patients themselves. And also can not modify their records. The patient can authorized the doctor to access their medical records, a patient can authorized more than one doctor to access his records at the same time.

(2) Doctors: Doctors also need to be registered in this system, but doctors chose doctor role during registration in order to get the authority of the doctor’s role. A doctor can simultaneously access multiple patient records. Before this, doctors need to make an agreement with his patients. After patients’ informing consents, the authority to access corresponding records will be set by the patients. The doctors can not access non-authorized patient’s record. Doctors can add new records for patients. But the same as patients, doctors can not modify the contents of the existing medical records,

(3) Administrator: The administrator manages the background of the system. Administrator does not visit any users’ personal information and medical records. Administrator can add or delete hospitals that participate in this information sharing system in a list. If a new hospital wants to join this system, then only the administrator can make the decision. Only when the hospitals had already been added into the system by the administrator, can achieve the information sharing with other hospital within this system. The administrator can also authorize the hospital to update the patients’ record. Such authorization requires the patients and doctors to reach an agreement. Administrator exists as a confidential third part outside of the patient and doctor. If medical records need to be modified, an agreement between patient and
doctor should be reached first. And then apply to the administrator. The corresponding operations are done by the administrator.

4.3 Selection of Tools and Models

In this section, the tools we chose to implement the EHR system are introduced. It includes the system architecture, RBAC model, database, programming language, compile software and database connection tool. All the tools and models were chosen to realize functions of an EHR system.

4.3.1 B/S Architecture

B/S: Browser/Server architecture, or WEB application. It’s 3-tier architecture, different from C/S (Client/Server 2-tier). In this architecture, user interface is realized by the WWW browser and few works done by Browser. The main part of work is done by Server. With this feature, users can visit texts, images and videos information through WWW browser. That information is generated by kinds of Web servers. Web servers are connected to the database servers. It send request to database servers to get the information stored in different databases. The databases are created in the database servers, so actually the information is stored in database servers. Compared with C/S, B/S architecture WWW browsers take the part of various Client applications using in C/S. Users just need a WWW browser generally they don’t need other user applications. Users can download applications from Web servers to local computers. Applications can be used to operate databases stored in database servers. The advantages of B/S:

(1) Distribution characteristics, query, browse and other services can be done anytime and anywhere.
(2) Easy to expand server functions by adding web pages.
(3) Easy to maintain. Users’ updates can be done by changing web pages.
(4) Easy to develop.
(5) Easy to share.

Figure 4. B/S Architecture
4.3.2 RBAC
RBAC, Role-Based Access Control. As introduced in the literature review part, it’s the authority distribution based on the roles. RBAC was chosen to realize the access control solution in this system.

4.3.3 SQL
SQL is short for Structured Query Language. The main function of SQL is to create connections to different databases. SQL was defined as a standard language for relational database management systems by ANSI (American National Standards Institute). SQL sentences can be used to search, update and manage data from databases. Most of the popular relational database management systems use SQL language.

4.3.4 SQL server 2005
SQL server 2005 is a relational database management system, developed by Microsoft. SQL server 2005 follows the SQL language standard defined by ANSI. SQL server 2005 database engine provides full XML support. Its application design model is combined with Windows DNA architecture. It can be used to develop Web applications. SQL server 2005 support English Query and Microsoft searching service. User friendly search and powerful search functions are included in its Web applications. Microsoft’s SQL server is developed for Windows NT. It focuses on Web application. A same database engine can be used in different platforms, from personal computers to large-scale servers.

The feature of its network makes it very suitable for the underlying database in the B/S architecture. Fully XML support makes it easy to operate by users through the browsers. SQL server 2005 is a mature database which is used in many different industries. It turns out to be a successful database.

4.3.5 JDBC
Java Data Base Connectivity (JDBC) is a Java API used to execute SQL sentence. It can provide unified access with a variety of relational databases. It’s constituted by a group of classes and interfaces written by Java language. Higher level instruments and interfaces can be built based on JDBC, which allows database developers writing database application. For example, using the JDBC API, there is no need to write an application for Sybase database, and write another application for Oracle database. The combination of Java and JDBC makes programmers don’t need to write different applications for different platforms.

JDBC can approve C/S and B/S models. In B/S model, commands are sent to the middleware first, and then the middleware send the SQL sentences to database. Database handles the SQL requests, and the result is generated by database, which is sent back to the middleware. Finally, users receive the result from the middleware.
Even different databases are used in different hospitals. JDBC makes it possible for users to access and operate different databases. This became the basis for data interoperability among different databases. JDBC can solve the information sharing problem among different databases.

4.3.6 **MyEclipse 6.5**
Eclipse is an open source Java development platform. Most of the users considered Eclipse as an IDE (Integrated Development Environment). But Eclipse also includes PDE (Plug-in Development Environment). This component is for the developers who aim at expand Eclipse. PDE allows them create instruments that seamlessly integration with Eclipse environment. MyEclipse is built based on Eclipse. It’s a Plug-in set, which is used to develop Java, J2EE. MyEclipse support Java, JSP, HTLM, SQL and JDBC, so it’s an ideal development platform. MyEclipse 6.5 is a classical version of MyEclipse. Collection of a large number of plug-ins makes this version of MyEclipse powerful to develop software.

4.3.7 **Java**
Java is an OOP (object-oriented programming) language. It’s developed by Sun Microsystem Company in 1995. Java now is a popular programming language, because of its generality, high efficiency, platform portability and safety. Java is highly recommended in distributed systems. Different from traditional C language, Java is more concise and more like human language.

Java is widely used in kinds of heterogeneous systems. Its OOP feature makes it suitable for the wide use of internet nowadays. Java program can be easily transplant to different platform.

4.3.8 **XML**
XML is short for Extensible Markup Language. It’s a markup language to make structural electronic documents. It can be used to mark data and define data structure. XML is suitable for Web transmission. XML provides a unified approach to describing and exchanging structures data which is independent from applications and providers.

4.3.9 **AES**
Advanced Encryption Standard (AES) is a block cipher standard. AES encrypted data block and key length can choose from 128 bits, 192 bits and 256 bits. AES encryption includes many rounds of duplication and transformation. Steps outlined below: (1) Key Expansion (2) Initial Round (3) Rounds, each round including Sub Bytes, Shift Rows, Mix Columns and Add Round Key (4) Final Round, there is no Mix Columns in the Final Round.
4.3.10 XMLHttpRequest
Users do not need to load the whole web pages when refresh the web pages using XMLHttpRequest. After loading the page, client can request for the data from server. Server receives the data and then sends data back to client in the background. The XMLHttpRequest object provides full access to the HTTP protocol, including the ability to make POST and HEAD requests, as well as ordinary GET request. XMLHttpRequest can be synchronous or asynchronous return to the Web server’s response, the content of the response can be returned by text or DOM text. XMLHttpRequest not only can be used with XML files, but also can used to receive kinds of text file. XMLHttpRequest object is a key element of a Web application architecture named AJAX.

4.4 System Functions
The functions of the system are divided into two parts, namely patients and doctors. In this section, most of the system functions are introduced. Patients and doctors functions have similar part. The similar part is to browse personal information and records. The main difference for patients and doctors can be simply explained to one-to-many and many-to-one. For patients, more than one doctor can diagnose the same patient. For doctors, a doctor can deal with multiple patients’ records.

4.4.1 Patient’s functions
When a patient login his account, there are two entrances: PersonInfo and Hospital. For the PersonInfo entrance, the patient checks his personal information or searches his records. In the ‘Personal information show’ page, the patient can choose checking his personal information or his records.

In the ‘personal information’ page, patient can update his account’s password and personal information. In the search page, this search function can be used to search specific records. Every time the patient goes to the hospital, the new record is generated, because of different diagnoses, different treatments, different diseases, different doctors and even different hospitals. However, the medical records are an important basis of diagnosis. Historical medical records play a very important role in supporting future disease treatment and health care, so all the patients’ past medical records will be used in his whole life.

Over a long period of time, a large number of records will exist in the patients’ account. When the user need to find specific records, the search function becomes very necessary. In this system, two search methods were used. The first one is to search based on the medical record number. The user can search for the appropriate medical records through the medical record number. In this search, patients can use the fuzzy search function. Patients only need to enter the part of the medical record number to get the result.
The second search method is based on the date of the creation of the medical record. There will be ‘start time’ and ‘end time’ to choose. Patients can choose the date which the medical records created in a calendar. The ‘start time’ and ‘end time’ may fix a certain period. Enter ‘start time’ and ‘end time’, then click ‘search’, all the records created in this period will be shown.

In the ‘Hospital’ page, patients can set authority. If a doctor wants to see a patient’s medical record, he needs to ask the patient to set the authority first. Patient can operate in his ‘Hospital’ page. Choose the doctor’s name, and then add this doctor to the authorized visitors’ list.

Figure 5. Patient’s Block Diagrams

Table 6 and Table 7 were designed to create user profiles and medical records. As shown in Table 6, there are eight items of user information. All items in the data type is ‘string’. In this system, all the users need to fill in this information. Part of this information is to verify the patient identity, including name, gender, date of birth and ID number. This is a real-name system, users have to use their ID number to register, and the personal information filled in by the user should be the same as the information corresponding to the ID number. This design is to prevent accounts from malicious registration. And the personally identifiable information helps the doctor to confirm the patient’s identity.

Table 7 is a basic design of medical record. The ‘Content of the record’ is the most important part. The doctor writes the patient’s diagnosis and treatment in this item. In the ‘Medicine’ item, doctor is required to fill in the patient’s drug. In the ‘Remark’ item, doctor can fill in some notes such as what should be paid attention in the daily life or the use of drugs. At last, it is the doctor’s name. It shows that the doctor takes
responsibility for this patient and corresponding treatment.

<table>
<thead>
<tr>
<th>Username</th>
<th>Data type (string)</th>
<th>Gender</th>
<th>Data type (string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phone</td>
<td>Data type (string)</td>
<td>ID Number</td>
<td>Data type (string)</td>
</tr>
<tr>
<td>Birthday</td>
<td>Data type (string)</td>
<td>E-mail</td>
<td>Data type (string)</td>
</tr>
<tr>
<td>Job</td>
<td>Data type (string)</td>
<td>Address</td>
<td>Data type (string)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hospital Name</th>
<th>Content of record</th>
<th>Medicine</th>
<th>Remark</th>
<th>Surgery</th>
<th>Doctor ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data type (string)</td>
<td>Data type (string)</td>
<td>Data type (string)</td>
<td>Data type (string)</td>
<td>Data type (string)</td>
<td>Data type (string)</td>
</tr>
</tbody>
</table>

4.4.2 Doctor’s Functions
There are two options in the doctor’s account. One is to view the doctor’s personal information, and the other is to search. It’s similar to patient’s function. In the doctor’s personal information option, the doctor can choose to update their account password. And then, the doctor can also choose to view their patients’ records. Similarly, a large number of patients’ medical records make doctors need medical records search function. In the search function, doctors have two search methods as the same as patients have. But, there is one difference. In the doctor’s search function, there is an ‘add new records’ function. Adding new records function is used in these two cases. One is a new patient that he has never had any medical record before. The doctor needs to create a new medical record for him. Another case is that the patients from one hospital to another hospital. The patient has record in the former hospital. But in the new hospital, the doctor makes diagnosis based on the former hospital records and his own diagnosis. It is also possible to create a new record.

![Figure 6. Doctor’s Block Diagram](image)
4.5 Implementation

4.5.1 Login Page
Before using the system, users need to login first. Traditional username and password have to type in the login page. After that, there is a drop-down menu. Users need to choose their own role, doctor or patient. There is a save username and password function in the login page. The user can check this option. After the first landing, the username and password are saved. There is no need to enter the username and password again in the future login. Finally, there are two buttons ‘login’ and ‘cancel’. If the user enter the correct username and password, and then click the ‘login’ button, the user will enter his user page.

![Login Page](image)

**Figure 7. Login Page**

4.5.2 Patient Part
This is the ‘PersonInfo’ page of the patient account. As Figure 8 shows below. Patient’s information is shown on the top of the page. There are some basic information, ‘name’, ‘age’, ‘address’ and ‘job’ are shown in the patient’s information.

In the patient’s personal information frame, there are two buttons. One is ‘updatepassword’ and the other one is ‘updatePersonInformation’. By clicking these two buttons, patient can enter the password modifies or personal information modify page.

Under the patient’s information, there are the records of this patient. Clicking the record number, patient can enter this record.

Each medical file has five basic data. It can be seen directly, it do not need to click the medical records to check. This can be convenient for patients to quickly browse. The basic information includes medical number, hospital name, patient’s name, responsible doctor’s name and the creation date of the record. In Figure 8, click the number in the ‘medicine record number’ list, then the record in shown on the right side.
Figure 8. Personal Information Show

Figure 9 shows the search frame. This is the search record’s number frame. At the top of the frame, there is a blank. Patient can type in the record’s number, and then click the search button to start search the records. As the Figure 9 shows, this is a fuzzy search typing in ‘2012’ in the search blank. The records that ‘2012’ is included in the record’s number will be shown.

Figure 9. Search Records on Record Number

This is another search interface. There are two options at the top of the interface ‘start time’ and ‘end time’. As shown in Figure 10, when users click on the space behind the option, there will be a calendar pop up. Month, Day and Year can be chose in the calendar. Users can intuitive select the record creation time and treatment end time, to confirm the corresponding medical records within the time frame.
4.5.3 Doctor Part

When doctor login this system, he can click the ‘updatePassword’ to change the password. Doctor’s password update function is the same as patients. Entering the update password page, the users need to enter the old password first, then enter the new password, and finally enter again. The new password is confirmed. In order to successfully update the password, the users must entered the same password twice. At last, click ‘submit’ to confirm that change.

Figure 11. Password Update Page

Figure 12 shows the doctor’s user page. Doctors can see a list of their patients’ records in their page. The doctor can view and only to view the records in the list. Not all the patients’ medical records are in the list. Only in two cases, the records are included in the list. One is that the records are created by this doctor. In the other case is that the doctor was already authorized by the patient. As long as the doctor clicks on the blue underlined record number he can enter the appropriate medical records.
the medical records list, each medical record has a corresponding hospital name, patient name and the date of creating medical record. These are convenient for doctors to browse and query the records quickly.

Figure 12. Doctor Information Show

Figure 13 shows the doctor’s medical records search interface. After entering the medical record number, doctor can see the corresponding medical records. Medical records include the patient’s basic information, and the most important thing, the content of the records. The record primarily aims at doctors for patients’ diagnosis, treatment and the use of medication.

Figure 13. Patient’s Record Show

4.6 Test and Evaluation

In this section, several tests are made to evaluate this system. Showing how this system satisfied with the users’ requirements.
4.6.1 Change on Record
As Figure 14 shows. If a doctor needs to check his patient’s record, he can just simply click on the record number, and then the detail of the record will be shown in the right side of the system.

![Figure 14. Record’s View in Doctor’s Account.](image)

As figure 15 shows, this is an original record, the descriptions and remarks are wrong. After the diagnosis, the doctor can change this record. There is a ‘apply cause’ on the bottom of the patient’s record. Doctor can write his application in this area and then click ‘apply’. The application will be sent to the system’s Administrator.

![Figure 15. The Original Record.](image)
Figure 17. Doctor’s Apply

Figure 18. Application Sent Successfully

Figure 19 shows the Administrator’s user interface. When the doctor sent the application to Administrator, there is an application notice in the Administrator’s user interface. As the figure shows, this is the doctor’s application notice. There is an ‘apply time’ on the top of the figure. Under the ‘apply time’ there are three options. The first one is the record number, showing which record need to be changed. If the Administrator agrees to this change, he can choose ‘pass check’. Then a ‘successfully’ notice will pop out which means it’s successfully change. If the Administrator doesn’t agree this change, he can choose ‘no pass’ which means the change is not allowed.

Figure 19. The Application Process in the Administrator

After the Administrator’s agreement, figure 20 is shown in the doctor’s interface. Now the doctor can change the record. The description is changed to the doctor’s diagnosis. The remark is also changed. After the change, click ‘update’ and then the update will be done.
4.6.2 Add new record

Doctor can search the patient’s depends on the file number. The file number is unique and fixed when the user registered. One patient has only one file number, but he can have many medical records.

After the search, the patient’s information and his corresponding records are shown. There are now 6 records of this patient. Doctor can add a new record for this patient by clicking ‘addNewRecord’ button.
Figure 23 shows a new record frame. Doctor can fill in the new record for the patient.

![Figure 23. Fill in New Record](image)

### 4.6.3 Background Tests

The background of this system is operated by the system administrator. In this section several tests were taken to evaluate the function of the system’s background.

![Figure 24. Administrator’s Interface](image)

Click ‘users’ list’, in this page administrator can delete or reset user’s password, the users including doctors and patients.
Click ‘add users’, administer can add user, by give out the username, password, type, and file number (if the user is patient).

Figure 25. Change User’s List

Click ‘add database’. After click, administer must set up the database.

Figure 26. Add User

Figure 27. Add Database

Figure 27 shows how to set a new database ‘hospital 9’. Administrator had to fill in this form to add a new database. Click ‘add database’, then can view the attach file in the local computer. Click ‘attach.bat’. Then administrator can add the database finally. If administrator wants to delete the database, click ‘delete database’. And choose ‘detach.bat’, the database will be deleted.
Figure 28. Set New Database

Figure 29. Choose Files

Figure 30 shows the records’ management function. In this part, all the records are shown. Administrator can choose to change the patient’s records. The Administrator also can control the user’s account. On the right side, this is the control function. Click ‘used’, then the account of the user can be used by the user. Click ‘non-used’, then the account is being blocked, the user can not use the account anymore.
4.6.4 Black Box Testing

Black box test also called function test. It’s mainly used to test the system’s functions. Wrong function, input output error, initialize error and end error can be found through the black box test. A completely black box test should considered all the input and output situations, thus innumerable situations have to test in the real test. It’s difficult to finish a completely black box test. So we carried out some targeted tests. Those tests focus on the main function of this system.

1. Function test
In the function tests, basic system functions are being tested. The test results are giving below.

<table>
<thead>
<tr>
<th>No.</th>
<th>Function</th>
<th>Expected outcome</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Update patient’s password</td>
<td>A successful notice popup.</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>Search on file number</td>
<td>All the medical records with the same file number show up.</td>
<td>pass</td>
</tr>
<tr>
<td>3</td>
<td>Search on date</td>
<td>All the medical records within the time range shows up.</td>
<td>pass</td>
</tr>
<tr>
<td>4</td>
<td>Add new record</td>
<td>A successful notice popup.</td>
<td>pass</td>
</tr>
<tr>
<td>5</td>
<td>Add users</td>
<td>User can login the system.</td>
<td>pass</td>
</tr>
<tr>
<td>6</td>
<td>Add hospitals</td>
<td>Hospital’s database can be found in the background system.</td>
<td>pass</td>
</tr>
<tr>
<td>7</td>
<td>Set authority</td>
<td>The doctor being authorized can access to the patient’s records.</td>
<td>pass</td>
</tr>
<tr>
<td>8</td>
<td>Change records</td>
<td>New records instead of the old records.</td>
<td>pass</td>
</tr>
</tbody>
</table>

2. Submit data without all field fulfilled test
In this part, we try to not fulfill the text areas. There should be reminder popup if user did not fill in all the text areas required to be filled in.
### Table 9. Non-fulfilled Test Result

<table>
<thead>
<tr>
<th>No.</th>
<th>Text field</th>
<th>Expected outcome</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Password change</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>Search on file number</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
<tr>
<td>3</td>
<td>Search on record number</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
<tr>
<td>4</td>
<td>Add database</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
<tr>
<td>5</td>
<td>Add user</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
<tr>
<td>6</td>
<td>Login</td>
<td>A reminder should popup.</td>
<td>pass</td>
</tr>
</tbody>
</table>

3. Change on data field test
Some corresponding changes should be show up when the text length change. To fit with the reading in text field.

### Table 10. Data Field Change Test Result

<table>
<thead>
<tr>
<th>No.</th>
<th>Text field</th>
<th>Expected change</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Change password</td>
<td>The background color will be change if the data out of range</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>Description</td>
<td>Seek bar should be dynamically change depends on the length of the text</td>
<td>pass</td>
</tr>
</tbody>
</table>
5. Result and Conclusion

5.1 System Interoperability and Access Control

In our system, the implementation of information sharing is combined with access control function. Patients have authority to set function using RBAC model. The doctor can not view the patient’s medical record unless he has been authorized by the patient. In other words, if the doctor has not been authorized by the patient, he can not view the records created by other hospitals and other doctors. Instead, he can only view the medical records created by them, which indicates that the information can not be shared between different hospitals and doctors. Therefore, to share information is the key function of the access control because the doctor can access to the medical records created by other doctors or other hospitals only when he is been authorized. This is precisely what we want to achieve. As Figure 14 shows, in the patient’s ‘hospital’ page, on the left side of this page, there is an optional name list of doctors. If a patient wants to authorize a doctor, he can find the doctor’s name in the list. Choose it and then click the double arrow between the ‘not selected doctor’ list and ‘selected’ list. In this way, the doctor will be added to the ‘selected’ list in the right side. When doctors are added to the ‘selected’ list, the doctor has been authorized by the patient. At this point, the doctor can access the patient’s relevant medical records.

When the patient wants to get rid of the doctor’s treatment, patients can remove the doctor’s name from the ‘selected’ list. Remove function is at the opposite way with add function. Select the doctor’s name in the ‘selected’ list. And then, click the left double arrow. This doctor will be removed from the ‘selected’ list, and then return to the ‘not selected doctor’ list. After that, the authority to access the patient’s medical records will be cancelled. The doctor will be not able to access to the patient’s medical record.

![Figure 31. Authorization](image-url)
5.2 Conclusion

This paper studies the information sharing and access control problems of EHR system. International and domestic literatures were reviewed, including the implementation of EHR system standards, and variety of access control models. After it focused on the problems faced with the current EHR system, then designed and realized a simple EHR system.

In this study, first of all it researched the information sharing, or called interoperability. The current medical information sharing is limited by the technology bottlenecks and the shortage of funds. In the research of the literatures, two main categories of information sharing were found, standardization and semantic sharing. Standardization refers to various local EHR system follow if the same information storage and transfer format and eliminating the difference between different systems. All patient information and medical records in the systems are in accordance with a uniform format. During the transmission, information send side will use a header file and the order of the information, which are agreed by both sides of the transmission. So the information recipient can accurately interpret the receiving information. This agreement is so called communication standards. HL7 CDA, HL7 v3 and openEHR are three most popular standards. These standards have been practiced for many years, and they are widely used. Another one is semantic information sharing. The semantic information sharing requires semantic tools or middleware technologies. Heterogeneous systems can communicate with each other by the use of semantic tools. In simple terms, it is like a translator between systems. Different information presentation ways can be converted to the expression that can be interpreted by the other system.

In this study, an attempt to use B/S architecture to design an EHR system is introduced. In the research part, the slowly development of EHR system was found.
Even though standards such as HL7 have done very well, it’s still difficult for using large-scale. This is mainly because the systems which are difficult to design. Use semantic tools to realize information sharing is easier than re-construct a new system. It can be compatible with existing systems. But, the reliability of semantic tools is still in doubt. Hospitals will never use un-accurate and un-reliable tools to share information. The misunderstanding will cause very serious consequences in medical field. B/S architecture can be a good solution to these problems. The user information does not need to be transferred between systems. Only to provide user information access interface is enough.

Varieties of access control models are also studied in this paper. RBAC, UCON, DRM and MAC models are included. Among those models, we found that some models can efficiently solve the problems of access control, and can be accepted by the system designers and users such as RBAC. After the research, RBAC model is considered to be suitable for promotion in the EHR system. In the B/S architecture EHR system studied in this paper, information sharing and access control can be combined together well. The system designer can considered both early in the design, which can greatly reduce the workload of the research and development.

Finally, based on the previous studies, an EHR system using B/S architecture was designed and realized. It has information sharing and user access control functions. The significance of this system is to make full use of the advantages of network and browser. Users can share information conveniently. JDBC provides a uniform interface with the access to different databases. The data in different databases can be unified access. It does not require designing corresponding program to use different databases. This system bypasses the complex data structure standards, and focuses more on information sharing itself. The information sharing was discussed in an entirely different angle. The system is a patient-centered system. Patient can easily access to their medical records, and have the rights to authorize doctors. The patient can become more proactive in this system.

The system provides a simple and useful template for the future design. Such a system does not require a lot of money and programmers to build. And it can generate very large benefits. The workload of medical staffs will be greatly reduced. It’s a simple system, which does not require a long period of training. Due to the features of this system, its scalability is good. It can provide an information sharing platform for entire city and even the entire country.
6. Recommendations for Future Work

In future studies, the combination of B/S and C/S systems can be focused on. The advantages of B/S system: (1) Easy to use. (2) Easy to develop. (3) Good at sharing. But there are also weaknesses, for example response too slow and simple in handle processes. In the C/S system, the client and server are directly connected. Therefore the response speed is fast. It has various forms of user interface. Thus, it can achieve complex processes. But, it has a weak distribution function, a poor compatibility and high technical requirements. This shows that the B/S architecture and C/S architecture can well complement each other. Combining these two architectures, it is achieved that the system can complete complex processes, response fast, has good compatibility and easy to expand.

This system needs a record system. When a doctor changes a patient’s medical record, the background management system shall record this change. The modifications and the name of the doctor also should be record. This record is available for the patients because patients have the right to know who changes their record, and what the change detail is. This can be evidence if some medical malpractices happened.

In this study, we focused on the information sharing between the patients and the hospitals. However, a complete EHR system should include not only the patients and the hospitals, many medical departments of the government should also be included. In future study, we can try to expand this system, which relevant government medical departments are included.

Because this study focused on information sharing, so there are only some important information is included in the patient’s record. In the future work, the record can be expand, more data can be stored. The patient’s medical data can be saved and generates charts, allowing users to see changes in their health more intuitive.

The medical images can be added into the patient’s record in this study. However, as technology evolves, multimedia health care is not limited to pictures, there are voice and video information. In future research, you can add more multimedia data to patient’s record, and give full play to the advantages of electronic storage.
7. References

7.1 List of References


### 7.2 Personal Contacts

**Guangxi Medical University**  
Contact person: Huang Ping  
Telephone: 008613877102629

**GuangXi Center for Disease Prevention and Control**  
Contact Person: Huang Shuhai  
Telephone: 008613877102629

**Guangxi touch High Technology Development Company**  
Contact Person: Li Bin  
Telephone: 008613977106820  
E-Mail: 214632461@qq.com
Guangxi Medical University
Contact person: Li Kehui
Telephone: 008613517880232
8. Enclosures

8.1 List of Acronyms

A:
ACM: Association for Computing Machinery
AMR: Automated Record
ANSI: American National Standards Institute
API:
ARRA: American Recovery and Reinvestment Act

B:
B/S: Browser/Server

C:
CDA: Clinical Document Architecture
CDC: Centres for Disease Control
CORBA: Common Object Request Broker Architectures
C/S: Client/Server

D:
DICOM: Digital Imaging and Communications in Medicine
DRM: Digital Right Management

E:
EPRS: Electronic Patient Record System

H:
HIPPA: Health Insurance Portability and Accountability Act
HL7: Health Level Seven
HL7 v3: Health Level Seven version 3
HTML: Hypertext Markup Language

I:
IDE: Integrated Development Environment
ISA: International Standards Association
J:
JDBC: Java Database Connectivity
JSP: Java Server Page

M:
MAC: Mandatory Access Control

O:
OOP: Object-oriented programming

R:
RBAC: Role-Based Access Control

S:
SOAP: Simple Object Access Protocol
SQL: Structured Query Language

T:
TCM: Tees Confidential Model
TCP/IP: Transmission Control Protocol/Internet Protocol

U:
UCON: Usage Control
UDDI: Universal Description Discovery and Integration

W:
WSDL: Web Services Description Language

X:
XML: eXtensible Markup Language
8.2 List of Full Papers


