The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 6, pp.173-180, Dec. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.6.173
JIIBC 2015-6-24

개인건강기록 시스템에서 개인 프라이버시 보호를 위한 보안 레이블 기법

A Security Labeling Scheme for Privacy Protection in Personal Health Record System

이명규*, 유돈식**, 황보택근***

Myung-Kyu Yi*, Done-sik Yoo, Taeg-Keun Whangbo*****

요 약 개인건강기록 기술의 출현은 인터넷 서비스의 이용 뿐 아니라 패러다임을 변화시키고 개인 맞춤형 서비스의 중요성을 강조하고 있다. 하지만, 개인건강기록 기술이 헬스케어와 융합되면서 사용자 개인정보 침해와 사용자의 민감한 의료정보가 유출되고 되는 문제가 증가되고 있다. 본 논문은 개인건강기록 시스템에서 프라이버시 보호를 위한 보안 라벨링 기법을 제안한다. 제안 기법에서 개인건강기록 데이터는 환자의 요청이나 보안 라벨 규칙들에 의해 자동적으로 분류된다. 제안된 기법은 접근제어, 보호대책을 구체적으로 명시하고, 통신 보안 정책에 의해 요구되는 추가적인 제한을 결정하는데 사용될 수 있다.

Abstract The advent of personal healthcare record(PHR) technology has been changing the uses as well as the paradigm of internet services, and emphasizing the importance of services being personalization. But the problem of user's privacy infringement and leaking user's sensitive medical information is increasing with the fusion of PHR technology and healthcare. In this paper, we propose a security labeling scheme for privacy protection in PHR system. In the proposed scheme, PHR data can be labeled also manually based on patient's request or the security labelling rules. The proposed scheme can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy.

Key Words : PHR, personal healthcare record, healthcare, wearable computer, HL7

Ⅰ. 서 론

최근 초고속 인터넷 기술의 발전과 개인 단말기의 보급 확산 및 성능 향상 등에 힘입어 언제 어디서나 개인의 건강관리를 간편하게 관리하는 스마트 헬스 서비스가 각광을 받고 있다. 개인 건강 기록(Personal Health Record, 이하 PHR)은 다양한 의료기관으로부터 제공되는 개인의 진료정보와 개인 스스로 기록한 건강기록을 통합적이고 포괄적인 관점에서 바라본 개인의 평생건강기록과 그 기록을 관리할 수 있는 도구를 말한다[1]. 궁극적인 PHR의 목적은 개인 건강에 관한 데이터와 문서를 원하는 시간과 장소에 환자나 보호자, 의료진과 같은 관련자들 사이에 효율적으로 접근하고 공유하며, 건강관리의 안전성과 품질을 높이고 치료의 효율을 향상시키는데 있다. PHR과 비슷한 개념으로 전자건강기록(Electronic Health Record, 이하 EHR)이 있다. EHR은

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 한국전자통신연구원
***정회원, 가천대학교 IT대학 컴퓨터공학과(교신저자)
접수일자: 2015년 11월 17일, 수정완료: 2015년 12월 7일
게재확정일자: 2015년 12월 11일

Received: 17 November, 2015 / Revised: 7 December, 2015 / Accepted: 11 December, 2015
***Corresponding Author: tkwhangbo@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

디지털 형식의 개인의 의료 기록을 의미한다. EHR은 컴퓨터를 사용하여 개인의 건강 기록을 저장하고 이용하며 일반적으로 컴퓨터에 저장된 것을 네트워크를 통해서 접근한다. 이러한 네트워크는 여러 곳이나 여러 소스에서 제공하는 EHR로 구성될 수 있으며 EHR에 포함되는 데이터는 환자의 신상명세, 의료 기록, 약품, 면역 상태를 포함한 알레르기 목록, 연구실 테스트 결과, X-레이 사진, 과금 기록 및 세부 지시 사항 등이 있다. PHR과 EHR의 주요 차이점은 PHR은 개인이 정보를 통제하지만 EHR의 경우에는 의사 또는 병원이 정보를 통제한다는 점이다. PHR은 언제 어디서나 평생 사용할 수 있으며 개인이 건강에 관한 여러 가지 결정을 내리는 데 사용할 수 있는 전자 형태의 건강 정보 자원이다. 과거 개인 활동정보는 센서나 웨어러블 디바이스가 존재하지 않아 수집이 불가능하였고, 진료기록의 경우 병원 내에서만 보관되어 있어 활용이 불가능했다. 하지만, 웨어러블 디바이스의 등장으로 운동량이나 혈압과 같은 일상생활에서 생성되는 활동 데이터를 측정할 수 있을 뿐 아니라, 병원 진료기록도 전산화되면서 개인 건강 관련 데이터를 통합적으로 수집하여 여러 가지 분석이 가능해지게 되었다. 이러한 분석을 바탕으로 개인 맞춤형 건강관리 서비스가 가능해졌다. 실제로 IBM, 애플 등은 병원 등과 제휴를 맺어 건강정보를 수집, 분석해 맞춤형 의료서비스를 전개할 준비를 하고 있다. PHR 시스템의 유형은 크게 3가지로 구분할 수 있다. 첫째는 독립형 PHR 시스템으로 EHR과 같은 의료기관의 정보시스템과 연결되어 있지 않고 독립적으로 존재한다. 예를 들면 PC기반의 소프트웨어나 인터넷 포털 사이트 형태가 될 수 있다. 두 번째는 제한형 PHR 시스템으로 의료기관의 정보시스템과 연결된 PHR 시스템을 의미한다. 마지막으로 연계형 PHR 시스템은 다양한 의료기관으로부터 필요한 정보를 전달받아서 분산된 다수의 서버 혹은 하나의 서버에 통합하여 저장하는 형태의 PHR 시스템이다. 서로 다른 기관으로부터 다양한 양식의 의무기록을 전송받아 저장하여야 하기 때문에 서식과 용어 등 공통의 표준화된 방식을 지원되어야 한다. 이와 같이 PHR은 다양한 장점을 가지고 있지만 아직 해결해야 할 문제들이 많이 있다. PHR은 민감한 개인정보가 포함되어있는 만큼 익명화되지 않은 상태로 활용된다면 프라이버시가 심각하게 훼손될 수 있다. 특히, 치료와 관련된 PHR은 의료법상 사용자에게 민감한 데이터로 취급되어야 하며, 민감하지 않은 데이터보다 엄격한 데이터 처리 정책이 적용되어야 한다. 본 논문은 사용자의 프라이버시 보호를 위한 보안 라벨링 기법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구를 설명하고, 3장은 제안된 기법을 위한 시스템 구성 및 제안된 보안 라벨링 기법에 대해서 설명한다. 4장은 제안된 기법의 실험 및 결과를 기술하며, 마지막으로 5장은 제안된 보안 라벨링 기법에 대한 결론을 도출한다.

II. 관련 연구

최근, PHR를 활용한 개인맞춤형 의료서비스에 대한 연구들은 다음과 같다. 2012년 8월에 미국 국가건강정보기술조정국(The Office of National Coordinator for Health IT, 이하 ONC)과 보훈청은 미국 내 모든 환자를 대상으로 확대하는 블루버튼 자동화 이니셔티브(Automate Blue Button Initiative)를 발표하였다[2]. 블루버튼(Blue Button)은 인터넷 상에서 개인 의료 기록을 열람하거나 다운로드 받은 후에 타 의료 기관에 제출할 수 있도록 하는 서비스로 보안 처리된 개인 의료 정보가 텍스트 형태로 제공된다. 블루버튼을 통해 모든 환자들은 클릭만으로 자신의 최신 의료 정보를 손쉽게 확인 가능하고, 환자가 의료 정보를 다운받아 타 기관에 제출할 필요 없이 기관 간 전송도 가능하다. 또한, 의료 서비스 제공자들도 환자 의료 정보를 전자 의료 기록으로 자동 전송하는 것은 물론 이메일, 헬스 케어 애플리케이션, 기타 환자가 지정하는 저장 공간으로 자동으로 안전하게 전송 가능하다. 향후 진료기록을 자동으로 전송해주는 기능(Push Service)과 서드파티 사업자가 환자 정보를 주기적으로 확인할 수 있도록 지원하는 기능(Pull Service) 제공할 예정이다. ONC는 의료 기록의 최신성이 보장됨에 따라 환자들이 건강관리에 더욱 신경 쓸 수 있을 것으로 기대하며, 실제로 블루버튼이 도입된 이래 보훈청에서만 70만 명이 넘는 시민들이 자신의 건강 정보를 다운로드 받은 것으로 확인되었다. 헬스볼트(HealthVault)는 마이크로소프트에서 운영하고 있는 대표적인 개인건강기록 통합 관리 서비스로 병원과의 연계를 통해 환자가 직접 자신의 건강 기록부, 각종 의료 관련 데이터를 휴대 단말기에서 관리하여 의료 기록 검색, 의사와의 상담, 자가 건강 검진 가능 서비스이다[3,4].

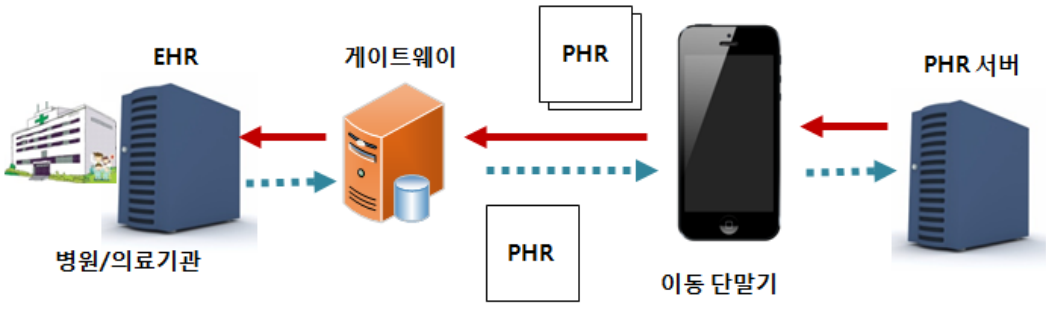

그림 1. PHR 시스템 구조
Fig. 1. PHR system architecture

환자는 심장 박동수, 혈압, 혈당, 활동량계 등에서 측정된 건강 관련 데이터를 앱에 포스팅하여 자신의 건강 상태, 일정 기간 동안의 변화, 추세 등을 통하여 자신의 건강 상태에 대해 세밀하게 파악 가능하다. 피트니스 단련 목적으로 할당량 목표 세우기, 과정 트래킹, 지인들과의 경쟁으로 동기 부여 등의 서비스도 제공하며 40개 이상의 협력업체들이 존재하고 있다. 헬스볼트의 개방 및 강화된 보안 플랫폼은 사용자가 웹기반 계정을 이용하여 다양한 헬스 케어 기관으로부터 나오는 의료기록을 저장할 수 있게 한다. 개인 또는 가족 전체의 의료기록을 관리할 수 있어 향상된 건강관리가 가능하다. 또한, 환자는 의사, 병원 외래 및 다른 의료기관으로부터 개인 의료 정보를 선택하여 헬스볼트에 저장할 수 있다. 헬스볼트 플랫폼은 처방, 수술기록, 퇴원 지시서, 검사결과, 방사선 사진, 보험정보, 응급연락처 등을 저장할 수 있다. 국내 대표적인 PHR 서비스는 서울 아산병원에서 제공하는 '내 손 안의 차트'가 있다. 환자는 '내 손안의 차트'를 이용하여 스마트폰으로 간편하게 진료이력, 질병이력, 알레르기, 검사결과와 같은 각종 서비스를 제공받을 수 있다. 주요 기능은 건강관리, 내 차트, 투약관리, 진료서비스 기능, 건강정보 등으로 구성되어 있다. 또한, '건강관리' 기능을 통해 환자가 주기적으로 관련 수치를 입력해 스스로의 질환을 관리할 수 있다. 입력된 수치는 병원의 EHR 시스템과 연동되어 병원 진료에도 활용될 예정이다. 하지만, 기존의 개발된 PHR 시스템은 환자의 프라이버시 보안에 취약하며 환자의 민감한 데이터에 대한 데이터 처리 정책이 적용되기 어렵다. 본 논문에서는 PHR를 활용하는 환자의 프라이버시 보호를 위한 보안 레이블 기법을 제안하고자 한다.

III. 제안된 보안 레이블 기법

그림 1은 본 논문이 제안하는 보안 레이블 기법을 위한 PHR 시스템 구성을 나타내고 있다. PHR 시스템은 환자 혹은 사용자를 위한 이동단말기, PHR 서버, 그리고 병원 EHR 시스템과 연결된 게이트웨이로 구성된다. 본 논문에서 PHR 문서는 XML(eXtensible Markup Language) 형태의 문서로 가정한다. 실제 CCR (Continuity of Care Record)[5]나 CCD (Continuity of Care Document)[6,7,8]과 같은 PHR 문서는 월드 와이드 웹 컨소시엄 (W3C)의 XML 스키마를 기반으로 하고 있다[9]. 개인 프라이버시 보호를 위한 보안 라벨링 주요항목은 표 1과 같다. 보안 속성은 Confidentiality(기밀성), Sensitivity(민감도), Integrity(무결성), Control(제어)의 하위항목으로 구성되며, 지정된 속성 값 중의 하나를 지정한다.

표 1. 프라이버시 보호를 위한 보안 라벨링 항목
Table 1. Security labeling item for privacy protection

주요항목	세부항목	필수/선택
기밀성 (Confidentiality)	없음	필수
민감도 (Sensitivity)	없음	필수
무결성 (Integrity)	신뢰(Confidence)	필수
	데이터 무결성(Data Integrity)	선택
	출처 보고(Provenance Reported)	선택
제어 (Control)	의무 정책(Obligation policy)	선택
	동의(Consent)	선택
	사용목적(Purpose of use)	필수

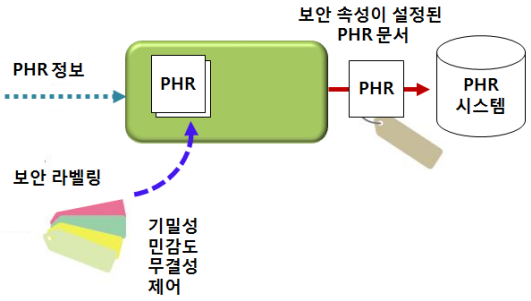

그림 2. 보안 라벨링 기법의 주요 개념
Fig. 2. Main concept for security labeling scheme

본 논문에서 제안하는 보안 레이블 기법은 그림 2와 같이 XML형태의 PHR 문서에 기밀성, 민감도, 무결성, 제어와 같은 보안 속성을 설정함으로써 개인 프라이버시를 보호하고자 함에 있다. PHR 문서는 연구 및 치료, 분석과 같은 다양한 목적을 위해 사용된다. 특별한 보호가 없는 환경에서 인가되지 않은 환경에서 사용자의 민감한 PHR 접근은 치명적인 위험에 노출 수 있다. 특히, 유전 정보, 정신 건강 정보, 미성년자 건강 기록과 같은 치료와 관련된 PHR은 의료법 상 사용자에게 민감한 데이터로 취급되어야 하며, 민감하지 않은 데이터보다 엄격한 데이터 처리 정책이 적용되어야 한다. 각 항목에 대하여 명시적인 동의가 필요하고 전문적인 접근권한을 가진 사용자들에 의해 수행되는 경우에만 처리가 허용되어야 하며, 건강관리 기관은 사용목적에 따라 필요한 경우에만 사용자의 접근을 제한해야한다.

PHR 서비스 담당자는 사용자의 동의 및 규정에 따라 어떤 환경에서 어떤 데이터를 접근할 것인지를 정책을 수립하고, PHR 정보 중에서 특별히 민감한 데이터에 대한 접근 및 분석을 수행하도록 요구 할 수 있다. 또한, 사용자 개인정보 침해를 방지하기 위해 의료진과 같이 매우 제한된 사용자만 PHR에 접근하도록 제한되거나 익명화된 사용자를 목표로 한 보호 장벽을 생성할 수 있다. 각 개별적인 수행 작업에 대해 자동화된 PHR 관리 및 개인정보 보호와 관리가 필요하다. 그림 3은 본 논문에서 제안하는 보안 라벨링 처리 흐름을 나타낸다. 사용자의 건강관리 어플리케이션에서 PHR 정보를 요청하면 사용자 단말기에 저장된 PHR정보나 병원 EHR을 통해 PHR 정보를 검색하여 XML문서로 변환한다. PHR문서에 보안 속성이 필요한 경우 민감도, 무결성, 제어와 같은 보안 속성이 설정한 후 PHR 문서를 어플리케이션에

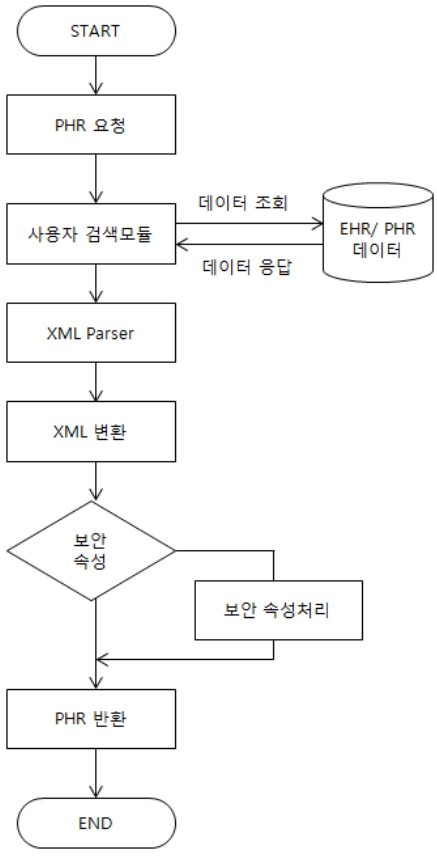

그림 3. 보안 라벨링 처리 흐름도
Fig. 3. Security labeling process flowchart

반환하게 된다. 프라이버시 보호를 위한 보안 라벨링 기법에서 보안 접근 정책은 표시된 자원에 대한 접근을 결정하기 위해 항목의 속성 값들을 참조하여 이루어지며, 제시한 보안 규칙에 따라 PHR를 입력 혹은 검색 시 자동적으로 분류 될 수 있다. 프라이버시 보호를 위한 보안 라벨링 항목에 대해서 자세히 설명하면 다음과 같다. 각 항목은 자원의 사용상의 제약을 나타낸다. 표시된 자원에 대한 요청이 있을 경우 접근 규칙을 표현하는 속성을 가지고 있으며 접근제어 정책에 사용된다. 기밀성은 가장 중요한 항목이며 PHR 문서의 기밀의 정도를 나타내기 위해 사용된다. 민감도는 사용자의 PHR 문서의 민감도를 나타내며 사용자의 요청 또는 전문적인 판단에 기초하여, 데이터 입력단계에서 수동으로도 표시 할 수 있다. 사용자가 특정 임상 사실이 민감하다고 판단되면 해당 속성을 부여할 수 있다. 무결성은 삽입된 데이터의 무결성을 표시하기 위해 사용된다. 제어는 취급 주의사

항으로 알려져 있으며, 두 개 혹은 그 이상의 시스템에서 PHR 문서가 교환될 때 취급주의 사항을 나타낸다. 예를 들어, 소스 기관은 다른 조직에 환자 데이터를 전송하기 전에 사용의 목적이 치료가 있음을 나타낼 수 있다. 또한, 수신시 익명화로 변환 의무를 나타낼 수 있다. PHR를 수신하는 의료 기관은 취급주의 사항을 준수해야한다. 각 항목은 다양한 속성 값들의 집합으로 이루어져있다. 사용자 혹은 PHR/EHR 시스템은 PHR 정보를 전송하기 전에 각 항목의 속성을 선택하여 입력해야 한다. 이 항목은 수신기관이 사용자를 식별 될 수 있는 방식으로 사용되거나 혹은 의도한 목적 외에 다른 목적으로 기록을 사용하는 것을 방지한다. 속성 값은 일반적으로 조건들로 구성되어 있으며 하나 또는 두 개의 속성 값으로 구성된다. 보안 레이블 기법은 PHR 문서에 대한 접근 권한이 설정 될 수 있도록 프라이버시 보호를 위한 표준적이고 계산가능하며 의미론적으로 상호 운영성 있는 수단을 제공한다. 또한, 적절한 접근 제어 결정은 보안 서비스의 각 계층에서 수행 될 수 있다. 각 요청은 요청자, 요청 된 리소스, 접근이 확립 될 수 있는지 여부를 결정하기 위해 각 필드에 필요한 속성과 제어를 지정한다. 시스템이 요청을 수신하면, 요청의 특성과 일치하는 정책을 찾아보고 그에 따른 결정을 적용한다. 보안 라벨링에서 지정할 수 있는 보안 속상 값에 대한 자세한 설명은 표 2와 같다.

표 2. 보안 라벨링 항목에 대한 매개 변수 값
Table 2. Parameter value for security labeling item

항목	하위 항목	속성 값	설명
Confidentiality	없음	Unrestricted , Low, Moderate, Normal, Restricted, Very restricted	기밀성 등급표시
Sensitivity	없음	Normal, Restricted, Very restricted	민감성 등급표시
Integrity	Confidence	Highly reliable, Reliable, Uncertain reliability, Unreliable	무결성 신뢰등급 표시
	Data Integrity	문자열	무결성 메커니즘 표시
	Provenance Reported	문자열	정보 출처표시
Control	Obligation policy	Anonymize, Deidentify, Encrypt, Mask, Redact, Pseudonymize	접근 제어 관련된 제어표시
	Consent	문자열	환자동의 여부표시
	Purpose of use	문자열	사용목적 표시

Ⅳ. 실험 및 결과

본 장에서는 제안된 보안 라벨링을 실제 구현하고 PHR 시스템과 연동을 테스트한다. 제안하는 보안 라벨링을 적용한 연동 테스트 순서는 다음과 같다. 사용자는 PHR 시스템에 접속하기 위해서 사용자가 소유한 계정의 아이디와 패스워드를 가지고 PHR 시스템에 접속한다. 사용자의 건강관리 어플리케이션을 통해 PHR 정보를 요청하면 사용자 단말기에 저장된 PHR 정보나 병원 EHR을 통해 필요한 정보를 검색한 후 XML문서로 변환한다. PHR 문서에 보안 속성이 필요한 경우 기밀성, 민감도, 무결성, 제어와 같은 보안속성을 설정한 후 XML 형태의 PHR 문서를 어플리케이션에 반환하게 된다. 데이터 연동의 용이성과 기능의 모듈화를 위해 Java로 구현하였으며, 구현환경은 표 3과 같다.

표 3. 구현환경
Table 3. Implementation environment

구분	구성요소	기종
하드웨어	CPU	Intel I5-6500 3.2GHz
	메모리	8GB
소프트웨어	운영체제	Window 8.1
	개발언어	Java, XML, JSP
	개발 플랫폼	Android Platform, JDK

보안 라벨 기법을 위한 스키마 구성의 예는 그림 4와 같다.

```
<xs:schema
 xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="PHRSecurityLabel">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Confidentiality" type="xs:string">
     <xs:simpleType>
       <xs:restriction base="xs:string">
       <xs:enumeration value="Unrestricted"/>
       <xs:enumeration value="Low"/>
       <xs:enumeration value="Moderate"/>
       <xs:enumeration value="Normal"/>
```

```
        <xs:enumeration value="Restricted"/>
        <xs:enumeration value="VeryRestricted"/>
       </xs:restriction>
      </xs:simpleType>
     </xs:element>
     <xs:element name="Sensitivity" type="xs:string">
      <xs:simpleType>
       <xs:restriction base="xs:string">
        <xs:enumeration value="Normal"/>
        <xs:enumeration value="Restricted"/>
        <xs:enumeration value="VeryRestricted"/>
        <xs:enumeration value="PatientDefault"/>
        <xs:enumeration value="PatientRequested"/>
       </xs:restriction>
      </xs:simpleType>
        .....
     </xs:element>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
</xs:schema>
```

그림 4. 보안 레이블 스키마의 예
Fig. 4. Example for security labeling schema

보안 라벨링 스키마를 이용하여 보안 레이블 기법이 적용된 PHR 문서의 예는 그림 5와 같다.

```
<PHRSecurityLabel>
 <Confidentiality>Normal</Confidentiality>
 <Sensitivity>Restricted</Sensitivity>
 <Integrity>
   <Confidence>Reliable</<Confidence>
 </Integrity>
 <Control>
  <Obligation policy>Encrypt<Obligation policy>
  <PurposeOfUse>Emergency treatment</PurposeOfUse>
 </Control>
</PHRSecurityLabel>
```

그림 5. 보안 레이블을 적용한 PHR 문서의 예
Fig. 5. Example for PHR document with security labeling

기밀성은 권한이 없는 개인, 단체, 또는 프로세스에게 사용이 가능하거나 공개되지 않는 정보의 속성을 의미한다. 그림 5의 경우 기밀성은 'Normal'로 설정되어 있다. 따라서, 해당 PHR 문서를 허가 없이 공개하는 경우 일반적인 피해가 발생하는 위험정도의 비낙인 건강 정보임을 나타내고 있다. 건강, 근로자 보상, 장애, 또는 생명보험과 같은 적용을 위한 공개적이며 비낙인 건강 정보가 포함되어 있음을 표시하며, PHR 시스템은 환자의 직접 치료를 위한 임상 치료의 목적을 위해만 접근이 가능하도록 해야 한다. 민감도는 객체의 속성에 의해 표시되는 민감한 정보를 표시할 때 사용된다. 그림 5에서 민감도의 속성은 'Restricted'로 설정되어 있다. 따라서, 해당 PHR 문서를 허가 없이 공개하는 경우 정보 주체에 대한 높은 위험을 표시하는 매우 민감하고 잠재적인 낙인 정보를 포함하고 있음을 나타내고 있다. 공중 보건보고서나 응급치료와 같이 관할 법에 의해만 공개될 수 있으며 정보 주체의 동의 지시문 혹은 좀 더 엄격한 법률조항을 준수 할 의무가 있음을 의미한다. 무결성의 경우 잘못된 정보의 수정 또는 파괴, 그리고 봉쇄부인 방지 및 신뢰성 보장에 대해 보호하기 위한 요구사항을 지원한다. 그림 5의 경우 신뢰는 'Reliable' 값으로 설정되어 있다. 따라서, 해당 PHR 문서가 명확히 기술된 사용목적을 인식되거나 적절한 정책에 의해 간주되는 신뢰성을 가지고 있음을 알 수 있다. 마지막으로, 제어는 기밀성, 무결성, 가용성을 보호하기 위해 정보 시스템에 대해 규정된 적용 관리, 운영 그리고 기술적 제어를 서술하고 있다. 그림 5의 경우 의무 정책(Obligation policy)은 'Encrypt'로 설정되어 있으며, 해당 PHR 문서는 적절한 암호화 처리가 필요함을 표시하고 있다. 또한, 사용목적(Purpose of use)은 'Emergency treatment'으로 설정되어 있으며, 응급 상황인 경우에 공개할 수 있음을 표시하고 있다.

V. 결 론

최근 의료 환경이 의료기관 중심에서 소비자중심으로 이동하고 있으며, 개인이 직접 자기 건강기록을 관리하고 언제 어디서나 접근이 가능한 PHR이 유헬스 환경 조성을 위한 발판이 될 것으로 전망되고 있다. PHR 활용을 통하여 의료기관은 환자에 대한 관리정보를 토대로 효율적 의료서비스 제공이 가능하며 개인화된 맞춤형 건강정보 제공이 가능할 것이다. PHR 서비스 활성화를 위해서는 개인 프라이버시 보안이 중요하다. 하지만, 대부분의 PHR 서비스는 개인 프라이버시 침해에 대한 보호가 미미한 실정이다. 본 논문은 PHR 시스템에서 개인 프라이버시 보호를 위한 보안 레이블 기법을 제안하였다. 제안기법에선 PHR 문서의 기밀성, 민감성, 무결성

에 따란 보안 속성을 설정할 수 있으며, 설정된 보안 속성을 통하여 접근제어와 같은 보안정책 설정이 가능하다. 본 논문에서 제안하는 보안 레벨링 기법은 PHR 정보를 활용하는 다양한 시스템에서 적용이 가능하며, 개인 맞춤형 의료서비스 및 건강관리 서비스를 제공하기 위한 접근제어, 보호대책을 구체적으로 명시하고, 통신 보안 정책에 의해 요구되는 추가적인 제한을 결정하는데 사용될 수 있다.

References

[1] Aizawa, K. ; Maruyama, Y. ; He Li ; Morikawa, C. , "Food Balance Estimation by Using Personal Dietary Tendencies in a Multimedia Food Log" IEEE Transactions on Multimedia, Vol.15, Issue: 8, pp2176-2185, 2013

[2] Chimezie Ogbuji, Karthik Gomadam, and Charles Petrie, "Web Technology and Architecture for Personal Health Records", IEEE Internet Computing, Vol. 15, No 4, pp. 10-13, July, 2011.

[3] https://www.healthvault.com

[4] Sunyaev A., Chornyi D., Mauro C., and Krcmar. H, "Evaluation Framework for Personal Health Records: Microsoft HealthVault Vs. Google Health", 43rd Hawaii International Conference on System Sciences (HICSS), pp. 1-10, Jan 2010.

[5] Sutanto, J.H.; Seldon, H.L.,"Translation between HL7 v2.5 and CCR message formats (For communication between hospital and personal health record systems)", In proc. of IEEE Conference on Open Systems , pp 406 - 410, 2011

[6] Vida, M.; Lupse, O.; Stoicu-Tivadar, L., "Improving the interoperability of healthcare information systems through HL7 CDA and CCD standards", In proc. of IEEE International Symposium on Applied Computational Intelligence and Informatics, pp. 157 - 161, 2012

[7] Lupse, O.; Vida, M.; Stoicu-Tivadar, L.; Stoicu-Tivadar, V., "Using HL7 CDA and CCD standards to improve communication between healthcare information systems", In proc. of IEEE 9th International Symposium on Intelligent Systems and Informatics, pp. 453 - 457, 2011

[8] Myung-Kyu Yi, Hee-Joung Hwang, "A Low Power Lifelog Management Scheme Based on User Movement Behaviors in Wireless Networks" The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 15, No. 2, pp.157-165, Apr. 30, 2015.

[9] Yun-Jeong Lee, Hyung-Deok Shin, "Effects of Contents Narrativity on the Related Contents Preference: Surveying on Korean College Students", Journal of the Korea Academia-Industrial cooperation Society, Vol. 16, No. 1 pp. 62-69, 2015

저자 소개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월 ~ 현재 : 가천대학교 IT 대학 컴퓨터공학과 연구교수
- TTA 유헬스 프로젝트그룹 개인건강정보 표준화 전담반 위원

<주관심분야 : u-Health, Big Data, Medical Informatics, Security, Ubiquious Computing>

유 돈 식(정회원)

- PhD (University College London, University of London)
- Rapporteur for ITU-D SG2 Q2/2 e-Health
- TTA 유헬스 프로젝트그룹 (PG419) 의장
- TTA 정보기술 융합 기술위원회 (TC4) 부의장

<주관심분야 : 개인건강정보 서비스 표준화, 의료정보 서비스 표준화, 디지털병원, 의학물리학의공학>

황 보 택 근(정회원)

- 1988년 CUNY 컴퓨터공학 졸업 (공학석사)
- 1995년 Stevens Institute of Technology 컴퓨터공학 졸업 (공학박사)
- 1997년 ~ 현재 가천대학교 IT대학 교수

<주관심분야 : 영상처리, 패턴인식, 컴퓨터그래픽스, 3D 게임엔진, 의료정보>

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0166-15-1007, 개인건강정보 표준화 및 상호운용성 기술 표준개발)