U-Healthcare 서비스의 개인정보보호를 위한 보안 요구사항에 관한 연구

채하나*, 송양의**
*동국대학교 정보보호학과
**동국대학교 컴퓨터공학과
e-mail: bindungi@gmail.com, redcroix@dongguk.edu

A Study on The Security Requirements for Privacy of U-Healthcare Service

Ha-Na Chae*, Yang-Eui Song**
*Dept of Information Security, Dongguk University
**Dept of Computer Engineering, Dongguk University

요 약

IT융합기술인 U-Healthcare 서비스는 건강관리, 질병 예방, 사후관리 등 필요한 의료 서비스를 의료기관외의 장소에서 언제 어디서나 서비스를 제공받을 수 있다는 점에서 각광을 받고 있다. U-Healthcare 서비스에서 다루는 대다수의 정보는 개인정보 중에서도 민감한 개인의 건강정보를 포함하고 있어 개인정보보호에 대한 사회적 요구가 높아지는 시점에서 유출에 대한 피해 우려는 더 커지고 있다. 본 논문에서는 U-Healthcare 서비스에서 개인정보를 보호받을 수 있는 보안 요구사항을 도출해낸다. 이 연구를 통해 U-Healthcare 서비스의 보안 수준을 향상 시키고 일반 개인정보보다 피해가 큰 개인건강정보의 유출을 예방한다.

1. 서론

IT 기술의 급속한 발전과 보급으로 인하여 다양한 IT 융합기술이 개발되고 있다. 그 중 하나로 의료서비스와 유비쿼터스가 접목된 U-Healthcare 서비스는 휴대용 단말기나 홈네트워크상의 장치를 이용하여 언제 어디서나 개인의 건강상태를 실시간으로 모니터링하고 건강관리 서비스를 제공하여 질병에 대한 관리와 건강 유지 및 향상을 목적으로 한다.[1] U-Healthcare 서비스를 이용함으로써 개인정보와 개인건강정보를 다루고 있기 때문에 정보 유출되어 사고 발생 시 그 피해는 일반 개인정보와 비교하기 힘든 파급력을 가지고 있다. 따라서 그에 상응하는 높은 수준의 개인정보보호 및 보안이 요구된다. 개인정보보호에 대한 사회적 요구가 높아지고 있는 현재 시점에서 개인정보보호는 U-Healthcare 서비스 활성화를 위해 필요하다.

그러나 의료분야와 IT분야에서 적용되는 지침이나 법규는 개인정보를 각각 다르게 다루고 있어 U-Healthcare 서비스에서 개인정보를 어느 분야에 맞추어 적용해야 하는지 그 처리 방법이 모호하다. 현재, 식품의약품안전청에서 제정한 '유헬스케어(U-Healthcare) 의료기기 품목별 허가·심사 가이드라인'[2]에서 개인의료정보 보안의 요구사항이 명시되어 있다.

본 논문에서는 U-Healthcare 서비스의 개인정보보호와 보안 수준의 향상을 위해서 국내에서 이루어지고 있는 각종 표준 지침 및 관련 법규, 인증 평가 등을 분석하여 기술적 영역 중심으로 보안 요구항목을 도출해낸다. 이를 통하여 효율적으로 정보보안 관리를 하고 개인건강정보의 유출을 예방하며, 의료분야와 IT기술 분야 사이에서 아직 정체성을 갖지 못한 U-Healthcare 서비스의 보안체계 구체화를 제안한다.

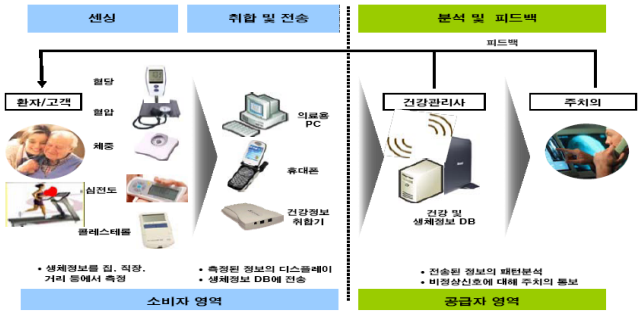
2. U-Healthcare 서비스와 개인정보

2.1 U-Healthcare 서비스

U-Healthcare는 그동안 많은 연구자나 기관에서 다양하게 정의되어 왔다. 이해의 내용에 따라 차이가 있을 수 있지만 유사한 개념을 내포하고 있다.

U-Healthcare(Ubiquitous Healthcare) 서비스는 IT, BT 등의 정보통신기술을 융합하여 의료산업에 접목함으로써 질병의 예방, 진단, 치료, 사후관리 뿐만 아니라 건강관리 등 필요한 보건의료서비스를 무구속·무자각 환경에서 언제어디서나 제공하는 것을 의미한다.[3] 기존 의료서비스를 지원하면서 서비스의 편리성을 높이기 위해 유·무선 네트워크를 활용하여 전자적 의료 정보 및 의료 예약관리 등을 제공한 e-healthcare 단계에서 한 단계 발전한 서비스이다. 당뇨병이나 고혈압 같은 꾸준한 모니터링이 필요한 만성질환 환자의 경우 병원 내에서만 치료가 가능하여 지속적으로 병원 진료를 받았었지만, U-Healthcare 서비스로 인하여 병원 외의 장소에서도 환자는 자신의 건강정보를 체크하여 상태를 전송하고 그 결과에 따라 진료를 받을 수 있도록 되었다. 앞으로의 발전 가속화를 고려해 봤을 때, U-Healthcare 서비스의 가장 중요한 조건은 환자의 상태를 정확하고 신속하게 전달 및 처리할 수 있는지의 여부이다.

U-Healthcare 서비스의 흐름을 살펴보면 아래와 같이 센싱, 취합 및 전송, 분석 및 피드백의 과정으로 구성된다.



(그림 1) U-Healthcare 서비스 흐름

센싱은 사용자의 생체 신호 및 의료정보를 측정하며, 취합 및 전송은 측정된 생체정보를 의미 있는 생체신호 성분만을 선택하기 위한 필터링과 생체정보 패턴분석과정, 이를 시각화하기위한 과정이다. 분석은 현재의 상태를 모니터링 할 뿐만 아니라 장기적으로 축적된 데이터로부터 건강상태, 생활 패턴 등을 나타내는 건강자료를 분석하는 과정이고 피드백은 분석된 건강 기지선이나 생활의 변화를 사용자의 행동변화, 경고 등으로 사용자에게 제공해준다.[4]

2.2 U-Healthcare 서비스와 개인정보의 관계

U-Healthcare 서비스의 기술은 의료 접근성을 높여 국민 건강에 뒷받침하는 긍정적인 측면과 더불어 발전함에 있어 그에 따른 위협 요소도 급증하고 있으며 그 위협요소들을 보완하기 위한 요구방안이 절실하다. 특히 U-Healthcare 서비스를 이용하게 될 경우, 정보통신망을 통해 전송 및 저장이 되는 개인건강정보는 개인의 생체정보뿐만 아니라 질병내력, 가족력, 신체적 특징 등을 포함하므로 유출된 개인건강정보를 통해 악의적인 목적으로 사용된다면 개인의 생명에까지 영향을 줄 수 있다.

U-Healthcare 서비스에서의 의료산업과 IT기술은 서로 다른 특성과 전문성을 요구하므로 서비스 제공자들은 어디서부터 어떻게 개인정보보호를 해야 할지 잘 모르고 있다.

개인정보와 관련하여 국내에서는 개인정보보호법[5], 의료법[6], 정보통신망 이용촉진 및 정보보호 등에 관한 법률[7] 및 식품의약품안전청에서 제정한 유헬스케어(U-Healthcare) 의료기기 품목별 허가·심사 가이드라인에서 권장하고 있는 개인건강정보 보호를 위한 기술적 요구사항[8]과 생체정보보호를 위한 가이드라인[9] 그리고 개인정보보호법에 따른 평가기준(개인정보영향평가)[10]이 있다. 최근에는 행정안전부와 보건복지부에서 개인정보보호법과 의료법이 중복이 되는 사안에 대하여 의료기관 개인정보보호 가이드라인[11]을 제공하였으나, 보안 요구항목은 구체적으로 명시되어 있지 않다.

본 논문에서는 유헬스케어 서비스 환경에서 기존보다 향상된 개인정보보호를 위한 요구사항을 제안한다.

3. U-Healthcare 서비스의 개인정보보호 요구

본 연구에서는 의료기관 개인정보보호 가이드라인을 참고하여 기존의 개인정보보안 표준 및 지침 등에서 제시된 보안 항목을 U-Healthcare 서비스의 범주의 맞춰 정리 및 재해석 하였다.

보안 영역은 개인정보의 수집, 이용, 보관, 파기 단계에 따라 보안 항목을 분류하지 않고 일반 정보시스템의 보안 요구사항에 따라 크게 관리적, 기술적 영역으로 접근하였다.

영역	요구항목
기술적	접근통제 및 접근권한관리, 개인건강정보의 암호화, 개인건강정보의 위/변조 방지, 침해사고 예방, 개인건강정보의 보존 및 폐기
관리적	정보자산의 분류, 내부관리계획 수립 및 시행, 침해사고 관리

<표 1> 개인건강정보 보안 영역

3.1 기술적 요구항목

기술적 요구항목은 접근통제 및 접근권한 관리, 개인건강정보의 암호화 등 5개 보안항목의 23개의 세부 통제 항목으로 아래와 같이 구체화 하였다.

3.1.1 접근통제 및 접근권한 관리

1) 개인정보를 취급하는 자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우, 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용해야 함.
2) 개인정보를 취급하는 시스템은 정보통신망을 통하여 불법적인 접근 및 침해사고 방지를 위해 침입차단시스템(FW), 침입탐지시스템(IDS), 침입방지시스템(IPS) 등의 정보보호 시스템으로 보호되는 구간에 설치·운영되어야 함.
3) 개인정보처리시스템에 대한 접근을 최소화하기 위하여 업무 수행에 따라 필요한 최소한의 범위로 업무담당자에 따라 차별화해야 함.
4) 개인정보처리시스템에 접근권한을 가진 담당자가 인사이동이 발생하여 변경 되었을 경우, 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소해야 하며, 접근 권한의 부여, 변경, 말소에 대한 내역을 기록하고 기록 내역은 최소 3년간 보관 및 관리되어야 함.
5) 개인정보가 집중되어 있는 데이터베이스의 경우 어플리케이션 서비스를 위한 서버와 분리되어 별도의 접근권한 관리가 이루어질 수 있어야 함.
6) 의료정보화시스템 데이터베이스는 응용서버와 논리적으로 분리하여 추가적인 접근권한 관리가 이루어지도록 구축해야 함.
7) 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인정보취급자별로 한 개의 사용자계정을 발급해야 하며 다른 개인정보취급자와 공유되지 않도록 해야 한다. 또한 개인정보처리시스템 이용 시, 하나의 계정으로 여러 사용자가 동시에 접속하지 못하

도록 제한 함.

8) 개인정보에 접근하는 취급하는 자는 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용해야 함. 비밀번호 작성규칙은 다음과 같으며 U-Healthcare 서비스를 이용하는 사용자에게도 권고해야 한다. 일정 횟수 이상 비밀번호 입력 오류가 발생할 경우 경고 메시지가 뜨고 사용 차단되도록 해야 함.

① 비밀번호 조합 및 최소 길이 설정 시, 영대/소문자(52자리), 숫자(10자리), 특수문자(32자리) 중 2개 이상을 조합하여 최소 10자리 이상이거나 3개 이상을 조합하여 최소 8자리 이상의 길이로 구성.

② 일련번호, 전화번호, 생년월일, 잘 알려진 단어 또는 키보드상에서 나란히 있는 문자열이 포함하지 않는 추측하기 어려운 비밀번호로 설정.

③ 설정한 비밀번호는 최소 6개월 주기로 변경해야 하며, 동일 비밀번호 사용은 제한.

9) 개인정보처리시스템 이용할 경우, 담당자의 공석 등으로 일정시간동안 사용하지 않을 경우 자동 세션 아웃되어 다른 담당자가 이용하지 못하도록 해야 함. 또한, 개인정보처리시스템 이용시간을 지정하여 이용시간 외에는 제한해야 함.

10) 저장 및 관리 중인 개인정보가 인터넷 홈페이지나 P2P, 공유 설정 등을 통하여 열람권한이 없는 자에게 공개 또는 외부에 유출되지 않도록 개인정보시스템 및 업무용 컴퓨터에 설정 기능 등을 제공해야 함. 별도의 개인정보처리시스템을 이용하지 않고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우, 업무용 컴퓨터의 운영체제(OS)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용해야 함.

3.1.2 개인건강정보 암호화

1) 개인건강정보가 정보통신망을 통해 송/수신될 때 SSL/IPsec 등의 기술을 이용하여 통신구간 암호화를 해야 함. 보조 저장매체 등을 통하여 전달되는 경우도 이를 암호화해야 함.

2) 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우, 암호화해야 함.

3) 비밀번호 및 바이오정보 등 본인임을 인증하는 정보에 대하여 복호화되지 않은 일방향 암호화(SHA-1, SHA-2 등)를 적용하여 저장해야 함. 개인건강정보를 암호화할 때에는 안전한 알고리즘으로 암호화(SEED, ARIA, AES 등)하여 저장해야 함.

4) 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우, 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장해야 함.

3.1.3 개인건강정보의 위/변조 방지

1) 시스템을 통하여 개인건강정보 취급 시 접근, 열람, 처리 등에 대하여 로그 기록이 남아야 함.

2) 개인정보 취급 담당자가 시스템에 접근하여 개인건강정보를 처리한 경우, 일시, 처리내역 등 접속한 로그을 기록하고 관리하여야 함. 이 로그 기록은 정기적으로 분리된 내부망에 존재하는 별도 저장장치에 백업하고 최소 6개월 이상 보관 및 관리하여야 함.

3) 시스템 접근, 처리 일시, 조회/인쇄/다운로드 등의 처리 내역, 접속 기록을 월 1회 이상 주기적으로 권한을 벗어나 과도하게 많은 개인건강정보의 조회에 대해 모니터링 해야 함.

3.1.4 침해사고 예방

1) 개인정보를 처리하는 시스템이 바이러스 및 악성코드에 노출되지 않도록 백신소프트웨어 등의 보안프로그램을 설치하고 보안 프로그램의 자동 업데이트 기능을 사용하거나 월 1회 이상 업데이트를 실시해야 함.
악성코드 관련 경보가 발령되거나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시해야 함.

2) 개인정보를 처리하는 모든 시스템에 대한 침해방지를 위해 시스템 취약점에 대하여 주기적인 진단을 수행해야 하며, 보안패치 적용 및 환경설정 조정을 통해 보완해야 함.

3) 개인정보를 처리하는 모든 시스템은 불법적인 조회나 접근이 발생하는가에 대하여 지속적이 모니터링이 되어야 함. 이와 관련한 모니터링을 위해 침입차단시스템, 침입탐지시스템 및 ESM 등의 정보보호 시스템을 활용할 것을 권고함.

3.1.5 개인건강정보의 보존 및 폐기

1) 개인건강정보는 진료정보에 포함되므로 의료법에 따라 사용자의 동의 없이 수집가능한 개인정보이며 의료법에서 정한 보존기간동안 보유해야 함. 신상정보는 최종 진료일부터 최소한 의료법상의 보존기간동안 보존해야 함.

2) 개인건강정보가 아닌 개인정보를 수집 시 보유기간이 경과하였거나 보유가 불필요하게 된 경우에는 5일 이내에 파기해야 함.

3) 폐기되어야 하는 개인건강정보는 복구되지 않도록 파쇄 또는 소각의 방법을 이용해야 함. HDD같은 저장매체에 관리되고 있는 경우, 물리적인 파괴, 자성을 이용한 제거(디가우징), 삭제 전용 프로그램 등을 이용해 완전히 파기해야 함.

3.2 관리적 요구항목

관리적 요구항목은 U-Healthcare 서비스를 운영하는 기관에서 개인정보보호의 기준을 세워 개인정보 침해위협을 줄일수 있도록 3개 보안항목, 7개의 세부 통제항목으로 아래와 같이 구체화 하였다.

3.2.1 정보자산의 분류

1) 개인건강정보 데이터의 중요도, 보호수준, 저장기간 등에 따라 분류해야 하며 각 데이터에 대한 이러한 내용을 목록화하여 관리 되어야 함.
2) 개인건강정보 등록 시, 중요 보안데이터에 대한 사용자 인증과 권한 관리 등 요구되는 보호수준이 결정해야 함.

3.2.2 내부관리계획 수립 및 시행

1) 상시 근무인원이 5인 이상인 기관은 개인정보보호책임자의 지정 및 개인정보보호 책임자/취급자의 역할과 책임 규정, 개인정보 안전성 확보에 필요한 조치, 개인정보 취급하는 담당자의 개인정보보호 관련 교육, 그밖에 개인정보보호를 위해 필요한 사항 등이 포함된 내부관리계획을 수립해야 함.
2) 개인건강정보를 위탁할 때, 반드시 위탁의 내용과 책임 등 개인정보보호법에 포함해야 하는 사항들을 담은 문서로 해야 하며 위탁 업무의 내용과 수탁자에 대한 사항을 인터넷 홈페이지나 기관 등의 보기 쉬운 장소에 게시하는 방법 등으로 공개해야 함. 또한 위탁자는 수탁자를 개인정보보호 관련 교육하고 감독해야 함.

3.2.3 침해사고의 관리

1) 개인정보 침해 규모를 정의하고 규모에 따라 적절한 보고체계를 수립하고 대응하여야 함. 사고 발생 시 피해를 최소화할 수 있도록 대응체계를 구축하여야 함.
2) 개인정보가 침해당했음을 확인하였을 경우, 정당한 사유가 없는 한 5일 이내에 사용자에게 유출된 개인정보 항목, 유출된 시점 및 경위, 유출로 인한 피해를 최소화하기 위해 사용자가 할 수 있는 방법 등에 관한 정보와 민원을 담당하는 창구와 신고, 접수방법 및 절차 등을 서면 또는 홈페이지 등을 통해 알려야 함.
3) 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책 마련과 필요한 조치를 하여야 함. 1 만 명 이상의 개인건강정보가 유출되면 5일 이내에 행정안전부나 한국인터넷진흥원(KISA), 한국정보화진흥원(NIA)에 신고해야 함.

4. 결론 및 향후과제

U-Healthcare 서비스에서 다루어지는 정보의 속성은 민감한 개인정보이며, 서로 다른 의료기관과의 연계로 정보공유가 빈번하게 이루어지고 있다는 점에서 개인정보 위협이 더욱 우려되고 있으며, 아직 U-Healthcare 서비스는 활성화 시작단계이고 의료산업과 IT기술 사이의 관련 법규에 대한 정체성이 미흡하므로 더 구체화해야 할 필요가 있다.

의료 및 건강관리 서비스와 IT 기술 분야는 서로 너무 다른 특성을 가지고 있어 U-Healthcare 서비스의 보안체계를 마련하기 쉽지 않다. U-Healthcare 서비스를 개발하는 개발자나 운영자는 IT시스템이면서도 개인건강정보를 다루고 있으므로 그에 상응하는 높은 수준의 보안이 요구된다는 것을 상기해야 하며, U-Healthcare 관련 업체는 보안의 필요성을 인식하고 요구되는 보안을 갖출 수 있는 보안 전문가를 보유하고 있어야 한다. 특히 의료와 관련된 개인정보 유출은 개인의 생명을 위협할 수 있는 심각한 취약점을 가지고 있음을 간과하지 말아야 하며, 이는 U-Healthcare 서비스 보안체계화 할 수 있는 필요충분조건이다.

본 논문은 국내에서 현재 사용되고 있는 각종 정보보안 표준 및 지침, 관련법규, 인증 평가 등을 분석하여 U-Healthcare 서비스에 맞추어 향상된 개인정보 보안 요구항목을 도출하였다. 이 항목들은 현실적으로 활용할 수 있도록 구체화 하였으며, U-Healthcare 서비스의 개인정보 보안 수준을 향상시키는데 도움을 줄 수 있을 것이다.

향후 연구에는 의료기관과 의료기관 사이의 연계성으로 인한 개인정보보호를 위한 요구사항에 접근해 보고, 국외에서 적용되고 있는 U-Healthcare 보안체계를 분석하여 좀 더 효율적으로 개인정보를 관리할 수 있는 방안을 제안할 예정이다.

참고문헌

[1] S. Y. Lee, K. B. Yim, K. J. Bae, Taeyoung Jeong and Jong-Wook Han, “Counterplan of Ubiquitous Home Network Privacy based on Device Authentication and Authorization”, Korea Institute of Information Security & Cryptology, 2008.

[2] 식품의약품안전청, “유헬스케어 의료기기 품목별 허가·심사 가이드라인”, 대한민국, 2010.

[3] T. M. Song, S. H. Jang, “u-Healthcare : Issue and Research Trends”, Korea Institute for Health and Social Affairs, Jan. 2011.

[4] 이봉근, 정윤수, 이상호, “유헬스케어 서비스 환경 내 개인정보 보호 모델설계”, 한국컴퓨터정보학회, 2011

[5] 행정안전부, “개인정보보호법률(법률 제10465호)”, 대한민국.

[6] 보건복지부, “의료법(법률 제11005호)”, 대한민국.

[7] 방송통신위원회, “정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제10560호)”, 대한민국.

[8] 한국정보통신기술협회, “개인건강정보 보호를 위한 기술적 요구사항(TTAK.KO-10.0304)”, 대한민국, 2008.

[9] 한국정보통신기술협회, “텔레바이오인식 보호 절차 - 바이오정보 보호를 위한 기술적·관리적 지침 (TTAS.KO-12.0034/R1)”, 대한민국, 2009.

[10] 한국인터넷진흥원, 행정안전부, “개인정보 영향평가 수행 안내서”, 대한민국, 2011.

[11] 행정안전부, 보건복지부, “의료기관 개인정보보호 가이드라인”, 2012

[12] 송지은, 김신효, 정명애, “u-헬스케어 서비스에서의 의료정보보호”, 정보보호학회, 2007