情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항

송 유 진*, 박 광 용**

요 약

최근 의료기술 발전에 따라 질병의 예방 및 관리에 대한 소비자의 요구사항이 증가하고 있다. 이러한 요구사항에 부응하기 위해 IT와 의료분야의 융합으로 u-헬스케어 서비스가 실현되고 있다. 언제 어디서나 의료서비스를 제공받을 수 있는 u-헬스케어 서비스의 활성화는 의료데이터의 공유 및 활용이 전제조건이 될 것이다. 그러나 의료데이터의 공유 및 활용으로 인해 의료정보에 포함된 개인정보, 병력정보 등의 프라이버시가 침해될 우려가 있다. 본 논문에서는 의료데이터의 공유 및 활용상에서 발생하는 보안 요구사항을 검토한다.

Ⅰ. 서 론

현재 우리 사회는 저출산과 사망률의 감소에 따른 인구의 고령화로 인해 의료서비스의 실질적인 수요가 증가하고 있다[1]. 또한 IT기반의 의료기술 발전과 함께 질병의 예방 및 관리가능성에 대한 소비자의 요구사항이 증가하는 추세이다.

이러한 요구사항에 부응하기 위해 의료와 IT의 융합을 통한 u-헬스케어 서비스가 실현되고 있다[2]. u-헬스케어 서비스는 의료서비스의 진화된 모델로서 공간적, 시간적 제약을 없애고 환자가 생활 공간 속에서 다양한 의료 센서 및 기기를 통해 수집된 생체 정보와 환경정보를 기반으로 중앙의 원격 의료 서비스 시스템을 통해 언제 어디서나 의료 피드백을 받을 수 있는 것이다[3].

하지만 u-헬스케어 서비스가 가능하기 위해서는 우선 기존 병원에서 종이나 수기로 관리하던 의료관련정보를 디지털화한 전자의무기록(EMR, Electronic Medical Record)을 구축해야 하고 의료정보의 공유 및 활용이 가능하도록 네트워크를 통합하는 전자건강기록(EHR, Electronic Health Record)으로 발전되어야 한다. EHR을 통해 진료정보에 대한 저장 뿐만 아니라 의료사고의 감소, 의사의 효율성 향상, 의료비용감소, 환자 관리의 표준화를 가능하게 하여 원격 진료, 건강관리 및 분석과 기록을 실현함으로써 의료의 질을 향상시킬 수 있는 기회를 제공한다.

하지만 대부분의 의료정보에는 개인정보, 병력정보 등 프라이버시를 침해할 수 있는 민감한 정보들이 포함되어 있다. 그러므로 의료데이터의 공유 및 활용상에서 발생하는 프라이버시를 보호해야 하고 보안 요구사항을 수립해야 한다.

본 논문에서는 u-헬스케어를 실현하기 위해 의료데이터 공유 및 활용 서비스를 위한 보안 요구사항에 대해 검토한다. 본 논문의 2장에서는 의료정보의 디지털화 및 통합관리에 따른 문제점에 대해 알아보고 3장에서는 의료정보 공유 및 활용상의 보안/프라이버시 보호에 대한 필요성을 검토한다. 4장에서는 의료정보의 공유 및 활용서비스를 위한 보안 요구사항을 수립하고 5장에서는 결론을 맺는다.

이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2009-0087849)
* 동국대학교 정보경영학과 (song@dongguk.ac.kr)
** 동국대학교 전자상거래협동과정 (freemickey@dongguk.ac.kr)

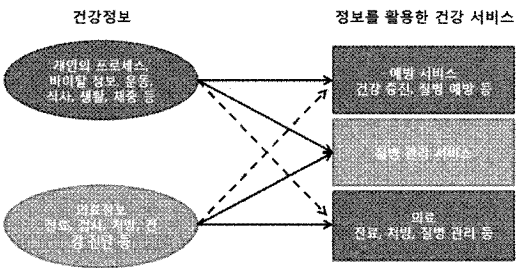
Ⅱ. 의료정보의 디지털화 및 통합관리에 따른 문제점

2.1 의료정보의 디지털화

u-헬스케어 서비스를 실현하기 위해 의료정보들은 디지털화 및 통합관리 되고 있다. 이에 따라 다음과 같은 사항들이 예상된다.

- 의료정보가 대량 축적되고 용이하게 열람할 수 있도록 되었다. 그러나 IT의 도입은 어떤 의미에서는 환자의 개인정보로서 의료정보를 침해할 위험을 증대시키고 있다.
- 인터넷이나 무선통신 기기를 이용한 의료 정보화를 통해 축적 및 교환되는 의료정보의 양이 폭발적으로 증가함에 따라 보호 대상 또한 급격히 증가될 것으로 예상된다.
- 의료정보의 안전한 유통과 관리를 위한 의료보안 서비스는 디지털 컨버전스에 따른 새로운 비즈니스를 촉진하고 완성하는 주요 요소로 인식되고 있다.
- u-헬스케어 서비스가 고도화 될수록 지능화된 의료 센서나 기기에 의한 개인 생체정보(바이탈 정보) 및 주변 환경 정보에 관한 모니터링이 가능해질 것이다. 또한, 유무선 네트워크를 통한 건강 정보의 공유가 확대됨에 따라 u-헬스케어는 개인 건강/의료 정보를 포함한 극히 개인적인 정보를 다루게 될 것이다.

향후에는 의료기관으로부터 제공되는 의료정보와 자택의 건강 기기의 개인 바이탈 정보가 하나의 PHR (Personal Health Record)[4]에 통합되어 관리·보관될 전망이다[그림 1][5].



〔그림 1〕 의료정보의 활용

이러한 경우 예방 서비스에서는 주로 개인의 프로세스·바이탈 정보가 필요하고 의료분야에서는 주로 의료정보를 활용한다. 여기서, 건강정보는 크게 ①의료정보, ②건강진단 정보, ③개인이 측정한 프로세스·바이탈 정보로 분류할 수 있다.

2.2 디지털화 및 통합관리에 따른 문제점

개인 의료정보를 디지털화하여 병원이나 의료기관에서 공유하여 사용하면 환자는 불필요한 검사를 생략할 수 있고 동일한 환자를 담당하고 있는 의사나 간호사는 그 환자의 의료정보를 공동으로 사용(Primary Care)할 수 있게 된다. 또한 의사는 진료 영상정보를 포함한 환자의 진단정보를 대형 의료기관에 전송하여 의견을 듣는 것도 가능하게 된다. 더 나아가 의료정보의 디지털화는 다른 환자의 진료를 위해 통계적 또는 임상실험, 역학연구 목적의 학문적 연구를 위한 데이터 수집이나 분석(Secondary Use)도 용이하게 된다.

하지만 의료정보의 디지털화는 다양한 장점이 있지만 환자 개인의 프라이버시 침해문제가 발생하게 된다. 즉, 의도적인 유출이 생기거나 의료정보의 거래, 부정한 열람 및 복제의 위험성에 직면할 수 있다. 특히 어떤 종류의 의료정보는 고용차별, 사회적 차별 등으로 인한 정신적 고통이라는 큰 불이익을 낳을 수 있게 된다. 예를 들어 HIV 바이러스 감염이나 정신 질환에 의한 고용차별을 들 수 있다. 향후, 이러한 프라이버시 침해로 인해 유전성 질환 유전자를 갖고 있거나 유전적 요인에 근거하는 고용차별이 생길 가능성도 있다.

의료정보의 프라이버시에 대한 위협요소 중에는 비공개되는 의료데이터 저장소에 저장·관리되는 의료정보를 무단으로 거래하고 유출시키는 것이다. 이러한 사례 중에 환자의 병력과 이름, 주소, 전화번호, 연령 등의 정보들이 전국의 약국과 건강 전문 업체로 판매되는 사례가 발생되고 있다. 예를 들면, 자궁암, 정신 분열증, 아토피성 피부염, 당뇨병 등의 병력을 가진 환자의 개인 의료정보 리스트가 전국의 약국과 건강식품 판매 회사에 거래되는 일이 발생되고 있다.

또한, 의료정보의 일부인 개인 유전정보의 유전자 분석연구에서도 프라이버시 보호 필요성이 중요시된다. 현재는 유전자 분석 연구가 대학, 연구소 등에서 이루어지고있만 향후에는 기업이 개인의 유전자 정보를 분석

하여 제약회사 등에 수탁하게 될 것이다[6]. 따라서 DNA의료분석에 수반하는 유전정보의 프라이버시 보호의 필요성이 높아지고 있다. 따라서 디지털화된 의료정보를 조합하여 익명화된 정보가 누구의 의료정보인지 식별하는 것을 방지하는 익명화 기술의 확립과 관리시스템도 필요하게 될 것이다.

의료정보의 비밀을 유지하기 위해 허가되지 않은 사람이나 단체는 그 정보의 내용을 알지 못하게 함으로써 정보 소유자의 인가를 받은 사람만이 접근이 가능하며 인가되지 않은 사람은 접근을 불가능하게 한다. 따라서 간호사, 의사 등 진료를 수행하기 위해 환자로부터 개인정보나 의료정보를 제공받을 필요가 있지만 환자로부터 얻을 수 있는 정보를 타인에게 불법적으로 공유/거래되어서는 안된다.

따라서 의료정보의 프라이버시 보호를 위해 부당한 고용 차별 · 보험 차별 · 사회적 차별로 연결될 수 있는 개인 의료정보의 유출방지, 타인에게 알려지고 싶지 않은 개인 의료정보가 무단으로 거래되지 않는 것을 보장해야 한다.

Ⅲ. 의료정보 공유 및 활용상의 보안/프라이버시 보호

3.1 의료정보의 공유 및 활용

현재 의료행위는 의사 한사람에 의해서만 행해지는 것이 아니라는 점이다. 즉, 의사와 환자 이외의 제3자, 보험자 단체, 행정, 의학연구자 등이 의료정보에 접근할 수 있다. 예를 들어, 병원에서는 의사의 지시를 받아 간호사와 약사를 비롯한 여러 직종의 의료 종사자가 환자에게 의료행위를 시행하고 있다. 게다가 전문적인 자격이 없는 사무직원과 위탁직원 등도 의료서비스에 관여하고 있다.

또한, 효율성 증진을 위해 의료시설 상호 제휴가 활발해지면서 시설 간 환자 정보의 교환 역시 문제가 되고 있다. 더 나아가 고령화 사회에 따른 보건 · 의료 · 복지의 통합적 제공이 강조되면서 개인정보의 보호문제는 더욱 대두된다. 즉, 어떤 환자가 의료서비스 이후에 건강관리 서비스를 이용할 경우, 해당 환자의 의료 관련정보가 보건이나 복지에 종사하는 사람들에게 활용될 수 있다.

이와 같이 환자에 대한 의료서비스 제공시 의사 이외의 많은 직종이 관여하며, 이로 인해 환자의 개인정보를 아는 자는 증가하므로 필연적으로 개인정보로서 의료정보가 침해될 위험은 커지게 된다. 특히 법률 등에서 비밀유지의무가 부과되어 있지 않은 의료 이외 직종의 관여로 인해 중요한 문제를 일으키고 있다.

한편, 정확한 진료를 받기 위해서 생체정보를 포함한 개인의 질병 내역이 공유되어야 한다. 이러한 정보들은 공유됨에 따라 중복된 검사와 의료조치가 반복되는 것을 막을 수 있고 선택적으로 다른 의료기관에 위임 및 제공된다.

3.2 의료정보 공유 및 활용상의 보안/프라이버시 보호 필요성

PHR 등 소비자 중심의 의료 서비스 제공을 위한 핵심 서비스로 개인의 건강과 관련된 정보를 평생 관리하여 예방 중심의 건강관리와 복지 및 건강증진 차원의 서비스를 제공하는 개념이다. 따라서 이를 실행하기 위해서는 안전한 의료정보의 공유/활용이 필수적이며 이를 안전하게 관리하기 위한 방법이 요구된다.

의료정보에는 크게 1차적인 정보와 2차적인 정보가 있다. 여기서, 1차적인 정보는 본인의 진료를 위해 의료정보를 사용하는 것이다. 따라서 환자자신의 치료나 예방을 위해 사용되기 때문에 자신의 동의가 암묵적으로 접근을 허가하고 있다. 따라서 1차적인 정보의 사용은 기본적으로 환자의 동의는 필요없다고 생각할 수 있다. 하지만 예를 들어, 성감염증과 같은 정보 등은 사전에 환자 자신의 동의를 얻어서 개인 식별정보와 분리하여 암호화할 필요성이 있다.

또한, 환자 자신을 특정 가능한 형태로 의료정보를 사용하는 것은 원칙적으로 본인의 의료를 목적으로 사용해야 하므로 의료정보의 사용과 범위를 담당의사, 간호사 및 환자의 가족 등 속성을 고려하여 설정되어야 한다.

2차적인 정보는 다른 환자의 진료를 위해 사용하거나 의학 연구를 위해 통계적 활용, 논문 작성, 학회 발표를 위한 사용, 의학 교육이나 의료 종사자의 연구목적에 의한 사용이다. 하지만 다른 환자의 진료를 목적으로 의료정보를 사용하려면 먼저 사전의 동의를 얻어야 하며 의료정보를 특정할 수 있는 개인정보는 익명화되어서 사용해야 하는 조건이 필요하다. 또한, 개인 의료정

보를 연구 목적으로 사용하는 경우에 의료정보가 익명화 되어 있는 상태라면 본인의 동의는 필요없게 된다.

한편, 의료-IT융합 활성화에 따른 의료데이터의 2차적인 사용 및 연구, 유전정보 등을 활용한 범죄수사에의 활용성이 커지는 반면, 이들 의료정보의 안전성에 대한 요구가 증대하고 있으며 이러한 필요성에 따라 IT기반의 의료정보를 안전하게 활용하고 공유하기 위한 기술적 보안 및 프라이버시 보호 장치가 마련되어야 한다.

또한, 의료정보가 디지털화되면서 EHR (Electronic Health Record) 등에 통합 관리 저장되고 의료진 또는 연구자에 의하여 부적절하게 이용될 경우, 개인의 프라이버시 침해로 이어질 수 있다. 이와 같이 개인의 프라이버시 정보인 의료정보는 안전하게 관리, 저장 및 유통되어야 한다.

의료기관 등에서 민감한 개인 의료정보를 데이터베이스에 보관하게 될 경우, 내부자 및 외부자로부터의 기밀성 유지가 필요하며, 또한 의료 서비스 내역 및 서비스 사용자에 대한 프라이버시 보호와 권한관리 유지가 필요하다. 특히, u-헬스케어에서 가장 문제가 되는 것은 개인의료 정보를 공유하는 것이다. 이에 따라, 개인 의료정보가 안전하게 공유되어야 하며 개인의 프라이버시 침해 문제가 발생하는 것을 방지해야 한다.

Ⅳ. 의료정보 공유 및 활용 서비스를 위한 보안 요구사항

u-헬스케어 환경에서 의료데이터 공유 및 활용은 서로 미리 관계가 설정되지 않은 불특정 다수가 참여한다는 고유의 특성을 갖는다. 또한, 미래에는 다수의 이질적인 의료데이터 서비스가 제공됨은 물론 환자나 민감한 데이터 소유자의 프라이버시 침해는 더욱 심화될 것으로 예상된다. 특히, 의료데이터 서비스의 공유 및 활용은 사용자의 의지와 상관없이 u-헬스케어 영역에서 일반화될 것으로 보인다.

의료정보는 개인정보 중 가장 프라이버시 보호가 필요한 정보 중 하나이며, 개인의 프라이버시에 대한 관심은 점차로 고조되고 있다. 그러므로 u-헬스케어 서비스가 활성화되기 위해서는 실시간 공유 및 활용되는 의료정보의 기밀성 보장, 접근 권한관리, 익명성 확보 등이 필요하다.

이와같이, u-헬스케어 환경에서 해당 환자의 치료와 진료정보를 포함한 u-헬스케어 데이터베이스 시스템에 저장된 각종 개인 의료데이터에 대한 프라이버시 보호, 정보 공유 및 활용의 문제가 발생하게 된다. 여기서, 프라이버시를 보호하고 기밀성 및 익명성 등을 유지하기 위한 요구사항은 다음과 같다.

- u-헬스케어 데이터베이스 시스템은 언제 · 어디서 · 누가 · 누구의 어느 의료정보에 어떻게 접근했는지 정확하게 관리되어야 하고 접근에 관한 추적성이 확보되어야 한다.
- 진료정보의 검색 및 이용시스템은 접근이력 정보 및 보안정책에 근거한 접근제어나 익명성을 제공하면서 검색을 허가해야 한다. 그렇지만 진료 업무에서 진료정보에 대한 접근권한과 임상연구, 교육업무 등을 위한 진료정보의 접근권한은 비록 동일 직원의 동일 환자정보에 대한 접근일 경우라도 달라질 수 있기 때문이다.
- 이러한 u-헬스케어 환경에서 의료데이터의 접근성을 개선하고 직원의 다양한 역할과 그 이력에 따른 접근제어 자유도를 유지할 수 있는 접근 권한관리 방식, 프라이버시 보호 및 데이터 보안 메커니즘이 요구된다.

4.1 기본개념

기본 요구사항을 수립하기 위해 u-헬스케어 데이터를 안전하게 관리하고 개인 의료정보의 프라이버시를 보호하기 위해 다음의 개념이 필요하다.

- 자기정보제어권
  의료정보가 생성, 공유, 활용됨에 있어서 자신의 의료정보를 제어할 수 있어야 한다. 따라서 프라이버시 보호를 위해 법적인 제재가 필요하거나 이러한 의료정보를 아무나 볼 수 없도록 암호화하는 방법이 있을 수 있다.
- 부정한 접근방지권
  의료정보를 접근할 때 허가된 사람만이 접근할 수 있지만 부정한 접근이 발생할 경우, 정보시스템에서 로그정보 등을 분석하여 불법접근을 방지하는 것이다.

① DB 투명성(Invisibility)

의료 데이터 사용자는 DB 투명성을 제공해야 한다.

〔표 1〕 요구사항

	기본방향	기본 요구사항
데이터 보안	· 기밀성 보장 · 무결성 보장 · 가용성 보장	의료 데이터는 안전하게 저장되어야 함
		외부 공격자의 침입을 통한 데이터가 불법으로 유출되어서는 안됨
		내부자에 의한 데이터 유출이나 실수에 의해 데이터가 유출되지 않도록 해야함
프라이버시 보호	· 익명성 보장 · 연결 불가능성 보장 · 식별 불가능성 보장 · 세밀한 접근 제어	의료 데이터는 익명으로 저장될 필요가 있음
		의료 데이터에 대한 접근제어 기능이 보장되어야 함
		의료 데이터에 대한 접근시 세밀한 접근제어 기능이 제공될 필요가 있음
권한관리 보호		의료 데이터는 안전하게 공유되어야 함
		의료 데이터 소유자의 소유권 등 지적재산권 보호가 필요함

여기서, DB 투명성이란 검색/입력/삭제/갱신 등의 쿼리를 처리할 경우, 데이터의 분산, 저장 및 전송방식과 무관하게 수행됨을 의미한다.

② 자기관리성 (Self Manageability)

사용자가 분산 저장된 의료데이터를 복원할 수 있고 저장된 데이터의 유지관리가 가능해야 한다.

③ 검색/입력/삭제/갱신 관리의 책임성(Responsibility)

의료 데이터 사용자는 데이터 관리시스템을 통해 제공되는 데이터의 검색/입력/삭제/갱신하는 과정에서

- 의료 데이터는 기밀성, 무결성 및 가용성이 보장되어야 한다.
- 정당한 권한을 가진 사용자만이 접근 가능해야 한다.
- 저장된 의료 데이터의 저장관리는 관리책임자와 보안관리자에 의해 수행된다.

  이때, 관리책임자와 보안관리자가 수행할 수 있는 직무를 다음과 같이 명확히 구분한다.
- 관리책임자는 의료데이터를 검색/입력/삭제 및 갱신한다. 또한, 의료 데이터의 백업/복구 등의 직무를 수행한다.
- 보안관리자는 의료 데이터에 대한 접근권한을 제어하고 안전한 분산·저장관리상의 직무를 수행한다.

의료 데이터에 대한 접근권한을 제어하고 안전한 분산·저장 관리를 위해 보안관리자는 다음과 같은 직무를 수행한다. 따라서 이러한 사항을 만족하게 하기 위해

- 의료 데이터 열람시 데이터의 불법 유출 및 안전한 관리를 위해 데이터에 대한 접근제어와 권한에 따른 승인이 요구된다.
- 의료 데이터는 소유자와 승인된 관리책임자에 의해 접근이 허용된다.
- 의료 데이터는 허가된 자만이 접근이 가능해야 한다. 즉, 권한이 부여되지 않은 자는 의료데이터의 검색이나 변경 등이 가능해서는 안된다. 이때, 사용자의 접근권한에 따라 의료 데이터의 공개 범위를 설정한다.
- 데이터 검색시 데이터의 기밀성 및 프라이버시를 유지하고 데이터 갱신시 데이터의 무결성, 가용성을 유지할 수 있어야 한다.
- 의료 데이터에 대한 불법적인 유통을 방지해야 한다.

4.2 요구사항

1) 의료 데이터에 대한 다음과 같은 데이터 보안 요구사항이 수립되어야 함.
   - 기밀성 (Confidentiality) 보장
   - 무결성 (Integrity) 보장
   - 가용성 (Availability) 보장

① 의료 데이터는 안전하게 저장되어야 함.

- 의료 데이터를 저장하고 있는 데이터베이스/시스템은 안전한 방법에 의해 보호되어야 한다.
- 안전한 저장 · 관리를 위해 데이터 암호화, 비밀분산 및 접근제어 기능 등이 보장되어야 한다.

  예) 의료영상 데이터의 경우 수십년 이상의 장기적인 저장이 요구된다. 수십년 이상의 장기적으로 저장할 경우 계산량적인 안전성에 근거하는 암호화 기법의 위험성이 노출되는 것도 고려해야 한다. 다시 말하면, 계산 처리 능력의 향상이나 암호 공격 수법의 발전을 고려하여 장기간 충분한 안전성을

확보할 수 있는 정보량적인 안전성에 근거하는 암호화 기법이 요구된다. 데이터베이스/시스템의 접근 제어 기능 뿐만 아니라 콘텐츠에 대한 암호화를 통해 기밀성을 확보할 수 있어야 한다. 이때, 제3자가 납득할 수 있는 안전성의 근거로 각종 안전성 평가를 실시한 결과를 나타낼 수 있어야 한다.

- 의료 데이터 유출 대책을 위해 데이터 보호기능을 시스템에 적용할 경우, 데이터 센터가 될 수 있는 스토리지 시스템의 신뢰성 대책으로써 백업이나 재해시의 데이터 복구기능 및 데이터 이상 감지 기능 등도 동시에 요구된다.
- 데이터에 대한 위변조가 없어야 된다.

② 외부 공격자의 침입을 통한 데이터가 불법으로 유출되어서는 안됨.
- 의료데이터의 불법 유출을 방지하기 위한 침입차단시스템, 침입탐지시스템 등의 보안 대책이 수립되어야 한다.

③ 내부자에 의한 의료데이터 유출이나 실수에 의해 데이터가 유출되지 않도록 해야 함.
- 암호화, 분산관리 등을 통해 유출이 되더라도 데이터를 이용할 수 없도록 보안상의 방법을 강구한다.
- 정규사용자에 대한 의료 데이터의 취득가능한 데이터량에 제한을 둔다.

2) 의료데이터 사용자의 프라이버시 보호를 위한 다음과 같은 요구사항이 수립되어야 함.
- 익명성 (Anonymity, Pseudonymity) 보장
- 연결불가능성 (Unlinkability) 보장
- 식별불가능성 (De-identification) 보장
- 세밀한(Fine-grained) 접근제어 기능 제공

① 의료 데이터는 익명으로 저장될 필요가 있음.
- 저장된 의료데이터는 데이터 식별자와 연결이 불가능해야 한다.
- 의료 데이터 소유자의 신원을 나타낼 수 있는 요소는 식별이 불가능해야 한다.

② 의료 데이터에 대한 접근제어 기능이 보장되어야 함.
- 허가되지 않은 사용자에 대한 접근제어가 필요하다.
- 인터넷을 이용한 통신외에도 단말기간의 통신 등 다양한 통신 경로가 존재함으로 기존의 접근제어와 같은 집중관리형의 정보 유출 방지대책 외에 분산관리형의 접근제어 대책이 필요하다.

③ 의료 데이터에 대한 접근시 세밀한 접근제어 기능이 제공될 필요가 있음.
- 의료데이터에 접근하는 자의 역할, 속성 및 환경 등을 고려한 접근제어가 필요하다.

④ 의료 데이터를 사용자의 역할에 따라 선택적으로 공개하는 기능이 요구됨.
- 동일 의료데이터내에서 열람 가능한 부분이 사용자의 역할에 따라 다르도록 설정함으로써 사용자의 역할 등에 따라 선택적으로 공개하는 기능이 요구된다.

3) 의료 데이터의 안전한 공유를 위해 다음과 같은 권한관리 요구사항이 필요함.

① 저장된 의료 데이터는 안전하게 공유·활용되어야 함.
- 의료 데이터는 데이터베이스에 저장되어 기업, 개인, 병원, 연구소 등의 서비스 요청으로 공유된다. 이때, 데이터를 공유, 활용할 경우 개인의 프라이버시가 침해되어서는 안된다.
- 공유된 의료데이터는 권한을 설정하여 안전하게 관리되도록 한다.
- 의료 데이터 공유에 대한 통제권 확보 즉, 권한을 적절하게 관리할 수 있는 방법이 제공되어야 한다.
- 의료데이터의 안전한 공유관리를 위해 등급별 보안 관리가 필요하다.

② 의료 콘텐츠 소유자의 소유권 등 지적재산권 보호가 필요함.
- 네트워크 사회에서 의료 콘텐츠 상품(데이터, 문서, 기타 창조적 작품)의 저작자 및 소유조직의 저작권을 보호하는 방법이 필요하다.
- 의료 콘텐츠의 경우, 권한이 없는 사람에게 불법으로 양도되어서는 안된다.

V. 결 론

지금까지 u-헬스케어 서비스를 실현하기 위한 의료 정보의 디지털화와 통합관리, 공유 및 활용상의 프라이버시 보호에 대해 언급하였다. 그리고 공유 및 활용상에서 발생하는 프라이버시 보호를 위한 보안 요구사항에 대해 검토하였다. 향후 이러한 요구사항을 만족시킬 수 있는 보안 및 프라이버시 보호 기술에 대한 검토가 필요할 것이다.

참고문헌

[1] 김홍근, 김윤정, "지식정보사회 의료 패러다임 변화와 정보보안", 정보보호 정책동향, 정책개발 06-05, 정보보호 이슈리포트, 2006.05

[2] 성건용, 장문규, 정문연, 김승환, 박수준, 박선희, "유비쿼터스 라이프케어 기술 동향", 전자통신동향분석 제22권 제5호 pp.24~24, 2007. 10.

[3] 송지은, 김신효, 정명애, 정교일, "u-헬스케어 서비스에서의 의료정보보호", 한국정보보호학회, 정보보호학회지 제17권 제1호 pp. 47~56, 2007.

[4] EHR 핵심공통기술 연구개발사업단 아키텍처팀, "PHR 현황분석서 V 0.91", 2008. 01.

[5] 日本 版PHR を活用した新たな健康サービス研究會, "「個人が健康情報を管理・活用する時代に向けて」", 2008. 03

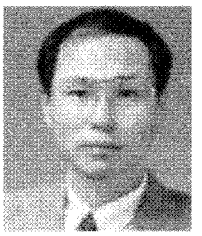
[6] http://www.zdnet.co.kr/Contents/2010/05 /09/zdnet-20100509164359.htm, 한국형 클라우드 서비스 진화한다, 2010. 05

〈著者紹介〉

박 광 용 (Kwangyong Park)

학생회원

2008년 2월: 동국대학교 전자상거래학과 졸업
2008년 3월~현재: 동국대학교 석사과정(전자상거래 기술전공)
<관심분야> 암호이론, 데이터 베이스 보안, 유비쿼터스 프라이버시 보호



송 유 진 (Youjin Song)

정회원

1982년 2월: 한국항공대학교 전자공학 학사
1987년 8월: 경북대학교 대학원 석사
1995년 3월: 일본 Tokyo Institute of Technology (동경공업대학) 정보보호학 박사
1988년~1996년: 한국전자통신 연구원 선임연구원
2003년~2005년: 미국 University of North Carolina at Charlotte 연구교수
2006년 7월~8월: 일본 정보보호대학원대학(IISEC) 객원교수
1996년~현재: 동국대학교 정보 경영학과/대학원 교수
2005년~현재: 동국대학교 부설 전자상거래연구소 소장
1998년~현재: 한국정보보호학회 이사
2006년~현재: 국제e-비즈니스학회 이사
2006년~현재: 한국사이버테러정보전학회 이사
2001년: ICISC2001 운영위원장
2003년: 하계CISC2003 프로그램위원장
2006년: CISC-S2006 공동 프로그램위원장
2007년: 한국정보시스템학회 추계 학술발표대회 공동 조직위원장
<관심분야> IT 융합보안(의료보안, 스마트그리드 보안) Cloud Security and Privacy, Secret Sharing, Context Aware Application Security