IE Interfaces
Vol. 20, No. 2, pp. 177-185, June 2007.

u-Health 환경에서의 정보보호 수준제고를 위한 보안 표준 개발

김동수[1] · 김민수[2†]

[1]숭실대학교 산업 · 정보시스템공학과 / [2]부경대학교 시스템경영공학과

Development of an Information Security Standard for Protecting Health Information in u-Health Environment

Dongsoo Kim[1] · Minsoo Kim[2]

[1]Department of Industrial and Information Systems Engineering, Soongsil University, Seoul 156-743

[2]Department of Systems Management and Engineering, Pukyong National University, Busan 608-739

e-Business in healthcare sector has been called e-Health, which is evolving into u-Health with advances of ubiquitous technologies. Seamless information sharing among health organizations is being discussed in many nations including USA, UK, Australia and Korea. Efforts for establishing the electronic health record (EHR) system and a nation-wide information sharing environment are called NHII (National Health Information Infrastructure) initiatives. With the advent of u-Health and progress of health information systems, information security issues in healthcare sector have become a very significant problem. In this paper, we analyze several issues on health information security occurring in u-Health environment and develop an information security standard for protecting health information. It is expected that the standard proposed in this work could be established as a national standard after sufficient reviews by information security experts, stakeholders in healthcare sector, and health professionals. Health organizations can establish comprehensive information security systems and protect health information more effectively using the standard. The result of this paper also contributes to relieving worries about privacy and security of individually identifiable health information brought by NHII implementation and u-Health systems.

Keyword: u-Health, information security, standard, national health information infrastructure

1. 서 론

e-Health라는 용어로 표현되는 의료 분야의 전자거래는 유비쿼터스 기술이 사회 각 분야에 활발하게 사용되기 시작하면서 u-Health라는 개념으로 발전하고 있다. 의료정보는 이제 개별 의료기관 내에만 존재하는 것이 아니라 인터넷을 통해 전송되어 여러 관련자들이 공유할 필요가 커지고 있다.

초고속 정보통신 인프라 수준이 매우 높고 IT 분야의 기술 수준이 높아짐에 따라 최근 국내에서는 의료정보화 수준이 급속도로 높아지고 있다. VAN 방식의 EDI 보험청구는 인터넷 기

본 연구는 보건복지부와 숭실대학교의 연구비지원에 의해 연구되었음.
†연락저자 : 김민수 교수, 608-739 부산시 남구 용당동 산 100 부경대학교 시스템경영공학과, Fax : 051-620-1546,
E-mail : minsky@pknu.ac.kr
2006년 12월 접수, 2회 수정 후 2007년 03월 게재확정.

반의 XML 보험청구 방식으로의 개선 방향에 대한 논의가 진행되고 있다. 보험청구 등과 같은 행정 관리 업무뿐만 아니라 진료 분야와 경영관리 분야 전반에 걸쳐 정보화가 진전되고 있다(Kim and Park, 2003).

또한, 환자 개인의 민감한 진료정보를 저장하고 있는 전자의무기록 시스템 도입이 가속화 되고 있다. 최근 국내외에서 의료 기관 간 의무기록의 공유를 목표로 의료정보의 표준화 및 상호운용성 확보를 위한 노력이 진행되고 있는데, 이는 전자의무기록이 개별 의료기관 차원에서 취급되는 것이 아니라 개인의 평생 전자건강기록(EHR: Electronic Health Record)으로 발전하는 것을 의미한다. 이러한 것을 가능하게 하는 국가 차원의 인프라를 총칭해서 NHII(National Health Information Infrastructure)라 부른다.

의료기관들 사이의 원활한 의료정보 교환과 공유를 위한 논의가 미국, 영국, 캐나다, 호주 등 선진국을 중심으로 진행되고 있으며, 우리나라도 전자건강기록(EHR: Electronic Health Record) 국가보건의료정보인프라(NHII: National Health Information Infrastructure) 구축 노력이 진행되고 있다. 이와 같이 u-Health의 등장과 의료정보화 발전으로 인해 개인 의료정보보호 문제가 중요한 이슈로 부각되고 있다. 즉, 의료정보화가 발전되고, 원격의료 및 재택의료의 확산과 유비쿼터스 기술의 의료 분야 적용이 확산되기 시작하면서 환자의 개인정보와 의료정보의 보호는 국가 차원의 보건의료정보인프라 구축을 위한 선결과제로 인식되고 있다.

특히 의료정보는 환자 개인을 식별할 수 있는 개인정보와 개인의 사생활보호 차원에서 매우 신중하게 취급해야 하는 민감한 진료정보 등을 포함하고 있으므로 의료기관의 정보보호 수준 제고를 위한 국가 차원의 노력이 요구되고 있다(Chae 2005). 이러한 배경에서 보건복지부에서는 개인건강정보의 보호에 관한 법률안 제정을 위해 노력 중이다.

본 연구의 목적은 u-Health 환경에서 개인의료정보를 취급하는 조직의 정보보호 수준을 제고하기 위한 의료정보보호 표준안을 개발하는 것이다. u-Health 및 국가보건의료정보인프라 구축의 방향과 정보보호 측면에서의 이슈를 분석해 보고 의료정보 취급 기관이 준수해야 할 보안 표준을 관리적, 물리적, 기술적 정보보호 대책으로 구분하여 제시하였다.

본 연구에서는 의료정보보호 표준안 개발을 위해 HIPAA 보안 표준과 BS7799 등의 국내외 관련 표준을 참조하였다(Joan Hash *et al*., 2005). 국내 의료 환경과 보안 수준에 부합한 표준을 개발하기 위해서 의사, 간호사, 의무기록사, 의료정보 전문가, 보안 전문가 등으로 구성된 보건의료 정보보호 표준화 분과위원회에서 의견 수렴을 하였다. 향후 보건복지부의 관련 법률이 제정되고 나면 국가 차원의 표준 제정으로 이어져 의료정보를 취급하는 기관의 정보보호 수준을 높이는데 기여할 것으로 기대된다.

본 논문은 다음과 같이 구성된다. 2장에서는 의료정보보호 표준안 개발의 필요성을 살펴보았고, 3장에서는 u-Health 발전과 정보보호 이슈를 분석하였다. 4장에서는 관리적, 물리적, 기술적 정보보호 방안 등으로 구성된 의료정보보호 표준안을 제시하였고, 5장에는 의료정보보호 표준 개발의 의의를 기술하였다. 끝으로 6장에는 본 연구의 결론을 제시하였다.

2. 의료정보보호 표준 개발의 필요성

전자상거래의 광의의 개념이라 할 수 있는 e-비즈니스는 거의 모든 산업에 영향을 미치고 있다. e-비즈니스화된 조직은 시장을 확대할 수 있으며, 비용 절감, 프로세스 개선, 상호작용 촉진 등의 장점을 기대할 수 있다(Efraim Turban and David King, 2003). 의료 분야에서도 이러한 기대 효과를 누리기 위해 다양한 측면의 e-비즈니스 도입이 진행되고 있다.

여러 문헌에서 의료 분야의 e-비즈니스 도입을 e-Health라는 용어를 통해 설명하고 있다(Eng, 2001; Eysenbach, 2001; Oh *et al*., 2005; Pagliari *et al*., 2005). 일반적으로 e-비즈니스 모델이 B2C, B2B, B2G 등으로 구분되는 것처럼 e-Health 모델 또한 B2B와 B2C, B2G로 구분할 수 있다. 그런데, 다양한 유형의 e-Health 모델의 실행에 있어서 정보보호 및 프라이버시 이슈가 중요한 문제로 등장하고 있다.

약품, 자재 공급자와의 B2B 거래와 같은 e-Procurement 혹은 공급망관리 측면에서는 일반적인 기업 환경에서와 동일한 유형의 정보가 교환되므로 이런 측면에서 의료 분야에서의 특별한 보안 이슈가 존재하는 것은 아니라고 볼 수 있다. 그러나 의료 서비스 제공자 사이의 상호작용과 같은 B2B e-Health 모델의 경우 진료 결과(clinical results)의 전송과 환자의 의무기록의 전자적 교환이 이루어지므로 보안 문제가 매우 중요하다.

또한, B2C 유형에 해당하는 환자와 의사간 상호작용의 경우도 의사와 환자 사이에 e-메일 교환과 전자처방전 전송, 인터넷을 통한 진료정보의 제공 등에 있어 보안 문제가 신중하게 고려되어야 한다.

국민건강보험공단, 건강보험심사평가원 등 정부기관과 의료기관 사이의 의료 보험 청구 데이터의 전자적 교환은 B2G로 볼 수 있다. B2G의 경우 비교적 보안이 강하다고 알려져 있는 EDI-VAN(Electronic Data Interchange- Value Added Network) 방식에서 인터넷 기반의 정보 교환 방식으로의 전환이 논의되고 있다. 1970년대에 등장한 EDI는 전자상거래의 시작으로 간주되고 VAN 기반의 EDI가 웹기반 EDI(혹은 인터넷 EDI), XML EDI 등으로 발전되어 왔다(Turban and King, 2003). 의료 분야에서의 프라이버시 보장과 정보보호 이슈에 대한 연구 및 관련 법제도의 정착은 EDI 도입과 매우 밀접한 관련이 있다.

미국에서 건강보험제도의 개혁과 행정절차의 간소화를 목표로 제정된 연방법률인 HIPAA(Health Insurance Portability and Accountability Act)의 주요 내용은 EDI 정착을 위한 제반 표준과 프라이버시 및 정보보호 표준안으로 구성된다(United States Department of Health Human Service). EDI 도입으로 강화된 의료

기관의 정보 활용과 관련 조직간 의료정보의 공유에는 반드시 정보보호 이슈가 쟁점으로 부각되므로 HIPAA에서는 정보화와 정보보호의 균형이라는 측면에서 프라이버시 규정과 정보보호 표준안을 포함하고 있다.

의료정보는 의사가 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 하여 연구 분석된 정보들을 포함하는 것으로써 진단과 그에 따른 치료행위 및 치료경과에 따른 면밀한 관찰 등을 모두 포함하는 전체과정에서 수집된 자료들을 의미한다(Chae, 2005). 의료정보는 병원의 내/외부적으로 다양하게 사용된다. 환자 진료 및 치료, 처방에 사용되는 것을 비롯하여 연구를 목적으로 한 조사, 법률적 자료(소송에 따른 증거), 의료비 청구 등에 사용된다.

의료정보는 개인의 프라이버시를 포함한 민감한 정보임에도 불구하고, 다양한 사람들로부터 정보의 공개 및 사용이 요구된다. 이러한 의료정보는 특히 OCS(Order Communication System), EMR(Electronic Medical Record) 시스템의 도입 등 의료기관의 정보화가 가속화되고 인터넷을 통한 정보 접근가능성이 확대되면서 의료정보의 손실이나 파손으로 인한 환자 안전에 대한 위협, 환자 진료정보나 개인정보에 대한 권한이 없는 자의 접근이나 정보유출로 인한 비밀성 침해, 필요한 정보서비스 제공의 불가 등 여러 가지 정보보호 리스크를 안고 있다.

환자 개인의 프라이버시에 대한 침해뿐만 아니라 정보의 무결성을 침해하여 부정확한 정보의 제공으로 환자 진료 시 위험을 초래할 수도 있다. 또한 정보보호 사고가 발생하게 되면 의료기관 등의 조직 평판 및 대중적 신뢰도 하락 등의 위험이 발생한다. 이러한 위험으로부터 환자의 의료정보를 보호하기 위해서는 의료기관 직원에 대한 보안 교육 실시와 마인드 제고가 필요하다.

2005년 2월에 발표된 전자의무기록의 프라이버시 리스크에 대한 조사 결과에 의하면 미국 성인의 70%가 데이터 보안 상 문제점으로 인해 개인의 보건의료정보가 유출될 수 있다고 우려하고 있다(P&AB and Harris Interactive). 동 조사에서 응답자의 69%는 전자의무기록 시스템을 통해 환자가 인지하지 못한 상황에서 건강정보 공유가 더 많아질 것을 우려하고 있으며, 47%는 전자의무기록의 장점보다 프라이버시 리스크가 더 크다고 생각하는 것으로 조사되었다.

환자의 개인의료정보를 보호하고 프라이버시 침해를 방지하기 위해서는 의료정보를 취급하는 의료기관을 포함한 모든 관련 기관의 정보보호 수준 제고가 필요하다. 국가보건의료정보 인프라와 EHR 시스템의 정착, 원격의료, 유비쿼터스 건강관리 등 가까운 미래에 도래하게 될 새로운 보건의료정보 인프라 및 서비스의 안전한 정착을 위해서는 의료정보에 대한 프라이버시 리스크를 줄이고 의료기관의 정보보호 수준을 제고하기 위한 국가차원의 관심과 노력이 필요하다.

의료기관들은 IT 투자 시 정보보호를 동시에 고려하여야 하며, 보안 시스템 구축 이전에 정보보호 규정과 조직, 보안 관리 체계 등을 우선 확보해야 한다. 새로운 취약점은 지속적으로 발생하며, 새로운 시스템 도입은 반드시 새로운 취약점을 유발하므로 시스템 개발 단계에서 보안 검토가 필수적이다.

이러한 점을 종합해 볼 때 국내에서도 개인 의료정보보호를 위한 종합적인 대책이 요구되고 있음을 알 수 있다. 정부에서 추진하고 있는 의료정보보호 관련 법제도의 제정 이후의 후속 작업으로 보안 표준안의 제정이 필수적이며, 이는 미국의 HIPAA 법안의 구성을 봐도 자명한 사실임을 알 수 있다(United States Department of Health Human Service).

HIPAA 보안규정은 전자적 형태(electronic form)로 된 의료정보에 적용되는 규정이다. 의료정보취급기관은 생성, 수신, 관리, 또는 전송되는 정보에 대한 기밀성, 무결성, 가용성의 보장을 통해 사전에 합리적으로 예측할 수 있는 위협 혹은 침해를 방지해야 한다. 또한 HIPAA 프라이버시 규정에서 허용되지 않는 정보의 예측 가능한 사용이나 유출을 방지해야 한다. 이를 위해 보안규정에서는 관리적 대책, 물리적 대책, 기술적 보안 대책을 포함하고 있다.

3. u-Health 발전과 정보보호

본 장에서는 u-Health의 발전 과정을 기술하고, u-Health 활성화를 위한 정책방향, 정보보호 이슈 등을 살펴 보았다.

3.1 e-Health에서 u-Health로의 발전

대표적인 유비쿼터스 서비스로 u-Health가 주목받고 있다. 최근들어 의료의 패러다임은 질병의 치료라는 전통적인 관점의 의료서비스에서 벗어나 건강한 상태의 지속적인 관리와 질병의 예방이라는 보다 적극적이고 확장된 개념으로 발전하고 있으며, 이를 뒷받침하는 기술이 바로 언제 어디서나 네트워크 및 컴퓨터에 연결되어 서비스를 활용할 수 있게 해 주는 유비쿼터스 기술이라 할 수 있다. 즉, 인터넷 및 정보기술의 발전과 맞물려 병의원 중심의 치료 개념에서 환자의 생활 공간에서의 건강관리 개념으로 의료서비스 패러다임이 변화하고 있는 것이다.

u-Health라는 개념은 인터넷과 정보통신기술을 활용한 건강관리 개념이라 할 수 있는 e-Health에 유비쿼터스 기술이 접목되면서 등장한 개념이라 볼 수 있다. 따라서 먼저 e-Health에서 u-Health로 이어지는 의료정보화 패러다임의 변화를 먼저 살펴볼 필요가 있다.

의료정보화 패러다임의 새로운 전환점이라 할 수 있는 e-Health를 보건복지부에서는 '정보통신기술을 활용하여 최대한의 의학지식과 환자정보를 제공함으로써 환자진료 및 개인건강관리 시에 효율적이고 합리적인 의사결정을 지원할 수 있는 정보체계'로 정의하고 있다. e-Health는 인터넷과 정보 기술의 발전으로 보건 의료서비스를 새로운 시각에서 조망하기 시작한 개념으로 Eng는 e-Health를 Content, Community, Commerce,

Connectivity, Care의 5가지 유형으로 구분하였다(Eng, 2001).

가장 발전된 e-Health 유형인 Care형 e-Health의 한 형태가 원격의료이다. 협의로 쓰일 때는 원격진료(telemedicine)라는 용어를 주로 쓰는데 정보통신기술을 활용하여 환자에 대해 의료서비스를 제공하거나 지원하는 것을 의미하며 환자에 대한 직접적인 진료, 치료 측면을 강조하는 개념이다. 광의의 개념으로 쓰일 때는 원격보건(telehealth)이라는 용어를 사용하여 환자에 대한 직접적인 치료뿐만 아니라 건강증진, 예방 등을 위한 교육, 공공 및 지역사회보건 등을 포함한다. 원격의료는 국내외적으로 의료시설과 인력이 취약한 산간벽지나 전쟁지역의 군대 등에서 유용한 수단으로 인식되고 있고 여러 사례를 통해 그 효과가 입증되고 있다.

앞에서 확인한 것처럼 의료서비스의 범위가 병원 내에서 환자의 생활공간인 가정이나 이동 중의 공간으로까지 확대되고 있으며, 유비쿼터스 기술이 보급되면서 e-Health는 u-Health라는 개념으로 발전하고 있다. 즉, 유비쿼터스 기술을 활용한 질병 치료 및 건강관리가 u- Health라는 용어로 표현되고 있다.

u-Health에서는 환자의 생활공간에서 여러 가지 생체 정보를 수집해 내기 위해 다양한 스마트 센서 및 유비쿼터스 네트워크가 필수적이다. 스마트 센서들은 환자의 의료정보를 수집하고, 집안 곳곳에 설치된 비디오 센서는 환자의 움직임을 관찰하여 환자의 상태를 체크한다. 개인의 생활공간인 가정이나 야외에서의 운동 상황이나 식이 상태 관련 정보를 수집하고 혈압, 혈당, 심전도, 체온 등 다양한 생체신호를 계측하여 데이터 센터로 전송되고, 의료 상담 시스템에 기록된 데이터는 병원의 의사나 간호사 등에 전송되어 환자에게 피드백을 하게 된다.

현재 국내외에서 다양한 u-Health 서비스 유형이 등장하였으며, 관련 제도가 정비되고 나면 여러 가지 u-Health 비즈니스 모델이 가능할 것으로 전망된다. 당뇨와 같은 만성질환의 관리에서부터 산모 및 태아의 건강관리, 심장질환 관리 서비스 등 다양한 분야에서 u-Health가 활용되고 있다. 최근에는 인피니온 사의 스마트 자켓, 조지아텍에서 개발한 스마트 셔츠, 비보메트릭스 사의 라이프 셔츠 등 각종 신체부착형 계측 장치가 건강관리를 위해 활용되고 있다.

3.2 u-Health 정착과 정보보호

이와 같이 국내외에서 다양한 u-Health 서비스와 비즈니스 모델이 등장하고 있는데 u-Health의 성공적인 정착 및 보급 활성화를 위해서는 해결해야 할 과제들이 많이 있다. u-Health는 보건의료와 정보통신기술 및 유비쿼터스 기술의 융합을 통해 등장한 개념이므로 법제도, 기술과 이용 환경에 걸쳐 여러 가지 해결해야 할 과제를 안고 있다.

다른 분야에서 유비쿼터스 서비스의 확산 및 성공의 경우와 마찬가지로 u-Health를 통한 국민 건강관리 향상 및 의료비 절감이라는 목표를 성공적으로 달성하기 위해서는 정부의 적극적인 역할 수행이 요구된다. u-Health가 비교적 빨리 정착하고 있는 나라로 인식되는 미국의 의료시스템과 우리나라의 의료시스템에는 큰 차이가 있다. 따라서 우리 정부는 이러한 의료시스템의 차이에 대한 이해를 바탕으로 u-Health 육성을 위한 정책을 개발하고, u-Health 발전에 걸림돌이 되고 있는 제반 환경적 요인을 정비할 필요가 있다. 우선적으로 의료정보보호 및 프라이버시 문제를 해결하기 위한 규정과 지침을 개발하고, 원격의료와 재택의료 관련 법제도 개선 등 기술 발전에 따른 관련법과 제도를 재정비할 필요가 있다. 아울러 유비쿼터스 기술을 이용한 새로운 의료서비스 제공방식에 대한 건강보험 수가 기준 마련 등 u-Health 시장이 형성될 수 있는 제반 여건을 조성해 나가야 한다.

u-Health에는 의료서비스 제공자(의사, 병원)와 환자, 보험자, 건강관리 업체 등 다양한 이해관계자가 참여하므로 상충되는 이해관계를 조정하여 u-Health가 활성화 될 수 있도록 사회적 분위기를 만들어 가는 것도 정부의 중요한 역할이라 할 수 있다.

무엇보다도, 유비쿼터스 건강관리의 보편화에 있어 장애요인으로 거론되는 국민 개개인의 프라이버시 보장과 의료정보보호 문제를 해결할 필요가 있다. 이 부분도 정부의 적극적인 역할이 필요한 영역이다. 환자의 의료정보에 관한 프라이버시 규정이 제정되어야 하며, 더욱 많아질 것으로 예상되는 의료정보 취급기관의 보안 의무사항에 대한 기준이 정립될 필요가 있다. 첨단 정보기술 및 유비쿼터스 인프라를 통해 고품질 개인맞춤형 서비스를 제공받기 위해서는 개인정보의 공개를 감수해야 하고 이는 개인정보 유출로 인한 피해 가능성이 높아진다는 것을 의미한다. 따라서 유비쿼터스 건강관리 시스템을 설계할 때에도 정보보호 문제가 설계 단계에서 고려되어 적용되지 않는다면 새로운 취약점과 유출 사고가 자주 발생할 것이다. 유비쿼터스 사회로의 이행에 있어 주요 장애요인인 정보보호 우려를 해소하기 위해서는 컴퓨팅 환경의 변화에 맞춰 현재의 법제도와 기술을 지속적으로 보완해야 한다.

유비쿼터스 환경에서는 흔히 전자태그라고 불리는 RFID, 각종 생체계측장비, USN(Ubiquitous Sensor Network) 등이 널리 사용되고 있다. 유비쿼터스 기술을 활용한 개인 건강관리 시스템 구축 및 운영 시 과다한 개인정보의 수집과 이용 논란을 유발할 수 있다. LBS(Location Based Service), 스마트카드 등 새로운 유비쿼터스 IT 기술로 인해 개인정보의 수집, 전송, 통합이 더욱 용이해 지고 있다(Kim and Kim, 2005). 유비쿼터스 환경에서 유의미한 서비스를 제공하기 위해서는 상황인지(Context Awareness)가 필요하므로 개인이 자신의 정보를 일정부분 공개하는 것은 꼭 필요하다고 볼 수 있다.

4. 의료정보보호 표준안

본 장에서는 u-Health 시대의 도래에 대비하기 위해 개별 의료정보취급기관들이 준수해야 할 정보보호 표준안의 개발 과정

및 개요를 서술하고, 관리적 보호방안, 물리적 보호방안, 기술적 보호방안, 조직 요구사항, 정책 및 절차 문서화 등 5가지 중분류 항목으로 구성되는 표준안의 세부 내용을 제시하였다.

4.1 표준 개발과정 및 표준안 개요

국내에서 의료정보보호를 위한 노력이 시작된 것은 비교적 최근의 일이며, 의료정보보호 관련법과 제도를 마련하는데 있어 HIPAA를 프라이버시 규정과 보안 규정을 많이 참조한 것이 사실이다. 본 연구에서 개발한 표준안 또한 HIPAA 보안 표준의 구성을 따르고 있다. 보건산업진흥원의 연구보고서에서 제안된 전자의무기록 보안 표준안 또한 이러한 구성을 따르고 있다(KHIDI, 2004; Chae, 2005). 현재 보건복지부에서 추진 중인 의료정보보호 관련 법안이 제정되고 나면 본격적으로 세부 표준안들이 확정이 될 것으로 예상되는데, 법안에도 HIPAA의 세 가지 분류인 관리적, 물리적, 기술적 정보보호 대책에 언급되어 있다. 따라서 본 연구에서도 의료정보보호와 관련한 여러 이해관계자들과 관련 기관 전문가, 정부관계자들의 의견에 기초해서 HIPAA 보안 표준을 토대로 의료정보보호 표준안을 개발하였다.

보건복지부에서는 국가보건의료정보인프라 구축을 위해 2004년부터 보건의료정보 표준화 위원회를 운영 중이다. u-Health 환경에서 제기되는 프라이버시 문제의 해결과 정보보호 기반 구축을 위해서 표준화 위원회 산하에 정보보호 표준화 분과위원회를 구성하였다. 이 분과위원회에는 의사, 간호사, 의무기록사, 의료정보 전문가, 보안 전문가 등이 참여하였으며, 본 연구에서 개발한 표준안은 국내 의료기관들의 경영환경과 실정에 부합할 수 있도록 이와 같은 공식 표준화 위원회를 통해 의견수렴과 검증 과정을 거쳤다.

본 연구에서 제시한 의료정보보호 표준안은 관리적, 물리적, 기술적 보호방안들과 조직 요구사항, 정책 및 절차의 문서화와 관련한 사항들로 구성된다. 이러한 의료정보보호 표준안의 전체적인 구성 체계는 미국의 HIPAA 보안 표준과 동일하다. 다만, 국내의 의료 체계와 관련 제도, 제반 의료 환경 등이 미국과 다르다는 점을 감안하여 세부 표준안을 마련하였으며, 여러 차례 분과 위원회를 개최하여 의견수렴을 거친 바 있다. 예를 들어, 관리적 보호방안의 세부 항목으로 정보 접근관리의 필수적인 요소로 의료정보변환소(Healthcare Clearing House) 기능 격리에 관한 조항이 있는데 이런 것은 우리나라의 의료 환경과 맞지 않는 것이다. 이와 같이 불필요한 내용은 제거하고, 또한 공식 HIPAA 보안 규정에는 포함되어 있지 않지만 필요한 사항을 추가함으로써 국내 의료 환경에 부합하는 표준을 개발하고자 하였다.

의료정보보호 표준은 관리적 보호방안, 물리적 보호방안, 기술적 보호방안, 조직 요구사항, 정책 및 절차 문서화 등 5가지 중분류 항목으로 구성되어 있으며, 각 중분류 항목은 여러 가지 소분류 항목으로 나누어진다. 각 항목별로 해당 항목의 목표를 달성하기 위해 의료정보취급기관이 수행할 필요가 있는 핵심활동과 이에 대한 설명, 그리고 핵심활동의 수행여부의 판단을 돕기 위한 예시질문으로 구성된다.

표준안의 세부적인 내용 구성에 대해서는 다음절부터 상세히 설명하였다.

4.2 관리적 정보보호 방안

관리적 정보보호 방안은 전자화된 개인의료정보를 보호하기 위해 필요한 보안 수단의 선택, 개발, 이행(implementation), 유지보수에 관한 사항과 대상 기관 인력의 정보보호와 관련한 행위를 관리하기 위한 관리적인 행동, 정책, 절차를 의미한다.

관리적 보호방안은 보안정책, 보안관리 프로세스, 보안담당자 확보, 직원보안, 정보접근관리, 보안인식제고 및 교육, 보안사고 대응절차, 비상계획, 평가, 사업 제휴 계약 및 기타 협정

표 1. 관리적 보호방안 예시 - 보안정책

핵심활동	설 명	예시질문
보안정책 수립 (필수)	◦ 의료정보취급기관의 경영목표를 지원할 수 있도록 보안의 법적, 규제적 요건과 전략적이고 조직적인 위험관리를 기술한 보안정책을 수립 및 문서화해야 함(목표, 적용범위, 요구사항, 역할 및 책임, 준수 의무 등)	◦ 기존 보안정책이 존재하는가? ◦ 보안정책에 위험관리가 기술되어 있는가?
정책의 체계 (권고)	◦ 상위 정책과의 일관성이 있어야 함 ◦ 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립해야 함 ◦ 상세 정보보호실행을 위해 정보보호 지침, 절차, 표준을 수립해야 함	◦ 정책이 일관적인가? ◦ 정보보호를 위한 지침, 절차, 표준이 정책에 포함되어 있는가?
정책의 공표 (필수)	◦ 정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달되어야 함	◦ 정보보호정책이 모든 관련 직원에게 전달되었는가?
정책의 검토 (권고)	◦ 정기적으로 정보보호정책의 타당성을 검토하여야 하며, 다음 경우에는 관련된 사항의 타당성을 추가로 검토해야 함. - 중대한 침해사고 발생 - 새로운 위협 또는 취약성의 발생 - 사업 내용 및 절차, 기술 기반구조, 임무 등의 대대적 변경 - 기타 정보보호 환경에 중대한 변화가 발생하는 경우	◦ 정기적으로 정책을 검토하는 절차가 존재하는가?

등 10가지 항목으로 구성되어 있다.

<표 1>은 관리적 정보보호 방안 가운데 보안정책에 대한 세부적인 내용을 보여 주고 있다. 지면의 제약으로 인해 전체 표준안의 내용을 논문에 포함하지는 않았으며 보건복지부의 관련 보고서(MOHW, 2006)를 참조하면 전체 표준안의 내용을 확인할 수 있다.

<표 1>에서 핵심활동은 개인의료정보보호 법제도를 준수하기 위해 필요한 주요 활동을 의미하며, 각 핵심활동은 필수 항목과 권고 항목으로 구분되어 있다. 핵심활동에는 구체적인 활동이 모두 포함되어 있지는 않으므로 의료정보취급기관에 적용할 때는 각 기관의 고유한 운영 방식을 고려하여 여러 가지 활동을 추가해야 할 것이다.

두 번째 열은 핵심활동에 대한 추가 설명으로 의료정보취급기관이 핵심활동을 이행하는 것을 돕기 위해 제시된 것이다.

세 번째 열은 제시된 핵심활동이 잘 고려되었는지 알아볼 수 있는 몇 가지 질문이 예시되어 있다. 예시질문은 가능한 질문을 총망라한 것이 아니며, 몇 가지 대표적인 질문을 정리한 것이다. 예시질문을 이용하면 개인의료정보보호와 관련된 보안 활동이 잘 이루어지고 있는지 초기 단계부터 검토할 수 있다.

예시 질문에 긍정적인 답변을 할 수 있다고 해서 의료정보취급기관의 보안 활동이 개인의료정보보호 법제도의 요구사항을 충족시킨다는 것을 의미하지는 않는다. 그러나 의료정보취급기관이 예시질문에서 제기된 사항을 고려하여 프로세스를 설계하였다면, 이 기관의 보안 활동은 개인의료정보를 보호하기 위한 올바른 방향으로 나아가고 있다고 볼 수 있다.

예시질문에 대한 부정적인 답변은 곧 의료정보취급기관이 개인의료정보보호 법제도를 충족시키기 위해 즉각적으로 적절한 행동을 취해야 함을 의미한다.

물론 예시 질문은 어디까지나 예시일 뿐이며, 의료정보취급기관의 보안 프로세스를 설계하고 평가하는데 필요한 질문은 각 기관의 환경에 맞게 수정하여 사용해야 한다.

다음의 <표 2>는 관리적 정보보호방안의 세부 항목별로 핵심활동 가운데 의료정보 취급기관이 반드시 수행해야 하는 필수적인 활동 목록을 보여 주고 있다. 필수 활동 여부의 선정을 위해 관련 전문가 및 의료종사자의 의견수렴을 거치기는 하였으나 추후 폭 넓은 의견 수렴이 필요할 것이다.

표 2. 관리적 정보보호방안의 보안 항목별 필수 핵심활동

범주	필수 핵심활동
보안정책	보안정책 수립, 정책의 공표
보안관리 프로세스	위험 파악, 위험 분석, 위험 평가, 위험 관리, 정책 및 절차 개발, 처벌 정책 개발 및 적용, 정보시스템 활동 보고 프로세스 개발 및 적용, 정보시스템 활동 감사 프로세스 이행
보안담당자 확보	보안 책임자 선정
직원보안	권한부여 및 감독 절차 이행, 정보 접근 허가 절차 수립, 접근 종료 절차 수립
정보접근관리	접근허가를 위한 정책 및 절차 실행, 접근권 부여 및 수정을 위한 정책과 절차 실행
보안인식 교육	N/A
보안사고 대응	보안사고 대응 및 보고 절차의 수립과 이행
비상계획	복구 전략 개발, 데이터백업계획, 재난복구계획, 비상 운영 계획 수립 및 실행
평가	N/A
사업 제휴 계약 및 기타 협정	계약서 또는 기타 협정 이행

4.3 물리적 정보보호 방안

물리적 보호방안은 대상 기관의 정보시스템 및 관련 건물, 장비들을 자연 재해나 환경적 위험요인, 불법적인 침입으로부터 보호하기 위한 물리적인 수단, 정책, 절차를 의미한다.

물리적 보호방안은 시설 접근통제, 단말기 사용, 단말기 보안, 장치 및 매체 통제, 장비보호 등 5가지 항목으로 구성된다. <표 3>은 물리적 정보보호 방안의 하나인 단말기 보안에 대한 핵심활동 및 예시 질문 등을 보여 주고 있다.

다음의 <표 4>는 물리적 정보보호방안의 세부 항목별로 핵심활동 가운데 의료정보 취급기관이 반드시 수행해야 하는 필

표 3. 물리적 보호방안 - 단말기 보안

핵심활동	설명	예시 질문
단말기에 대한 모든 물리적 접근방안 식별(권고)	◦ 직원 및 기타사용자가 단말기(컴퓨터 터미널, 노트북, PDA 등)에 접근할 수 있는 여러 가지 방법을 문서화해야 함.	◦ 단말기가 설치된 모든 장소가 목록으로 문서화되어 있는가? ◦ 단말기가 공개적인 장소에 설치되어 있는가? ◦ 노트북이 단말기로 사용되는가?
접근의 각 유형별 리스크 분석 (권고)	◦ 어떤 접근 방법이 보안에 가장 큰 위협이 되는지 파악해야 함.	◦ 단말기가 데이터의 허가되지 않은 사용 및 수정, 절도 등이 쉬운 장소에 설치되어 있는가? ◦ 현재 접근 설정을 수정할 수 있는가?
단말기를 위한 물리적 보안 수단 마련 및 실행 (필수)	◦ 단말기를 통한 부적절한 개인의료정보 접근 가능성을 최소화하기 위한 보안 수단 및 물리적 보호대책을 이행해야 함.	◦ 어떤 보호대책이 마련되어 있는가? 보호대책의 예로는 문 잠금장치, 화면보호기, 카메라, 경비원 등이 있다. ◦ 물리적 보안 향상을 위해 단말기가 재배치 될 필요가 있는가? ◦ 직원은 보안 교육을 받았는가?

표 5. 기술적 보호방안 - 네트워크 통제

핵심활동	설 명	예시 질문
접속시간 제한 (권고)	◦ 위험도가 높은 응용 프로그램에 대하여 접속시간을 제한 할 수 있어야 함.	◦ 위험도가 높은 응용프로그램은 무엇인가? ◦ 각 응용프로그램에 따라 적절한 접속시간이 설정되어 있는가?
네트워크 사용정책 (권고)	◦ 사용자들은 특별히 사용이 허가된 서비스에 대해서만 직접 접근 권한을 가져야 함.	◦ 사용이 허가된 서비스는 무엇인가? ◦ 사용자에게 접근 권한을 부여하는 절차가 존재하는가?
정보와 소프트웨어 교환시 보안관리 (권고)	◦ 전자우편을 송수신하거나 전자상거래 또는 공개서버 사용을 제한해야 함.	◦ 전자우편 송수신을 제한하는 절차가 존재하는가?

수적인 활동 목록을 보여 주고 있다.

표 4. 물리적 정보보호방안의 보안 항목별 필수 핵심활동

범주	필수 핵심활동
시설 접근통제	시설 보안 계획 수립
단말기 사용	N/A
단말기 보안	단말기를 위한 물리적 보안 수단 마련 및 실행
장치 및 매체 통제	개인의료정보의 최종 폐기를 위한 방안 실행, 전자적 미디어의 재사용을 위한 절차 마련 및 실행, 하드웨어 및 전자적 매체를 위한 책임자 선발, 데이터 백업 및 저장 절차 마련
장비 보호	N/A

4.4 기술적 정보보호 방안

기술적 정보보호방안은 전자화된 개인의료정보의 보호와 접근 제어에 사용되는 기술, 정책, 절차를 의미한다. 기술적 정보보호방안은 접근통제, 감사통제, 무결성, 인증, 전송보안, 네트워크 통제 등 6가지 항목으로 구성된다. <표 5>는 기술적 정보보호 방안의 하나인 네트워크 통제에 대한 핵심활동 및 예시 질문 등을 보여 주고 있다.

다음의 <표 6>은 물리적 정보보호방안의 세부 항목별로 핵심활동 가운데 의료정보 취급기관이 반드시 수행해야 하는 필수적인 활동 목록을 보여 주고 있다. 기술적 정보보호방안의 경우 감사통제, 인증, 네트워크 통제 등 필수적인 핵심활동이 없는 보안 항목이 여럿 포함됨을 알 수 있다.

표 6. 기술적 정보보호방안의 보안 항목별 필수 핵심활동

범주	필수 핵심활동
접근통제	모든 시스템 사용자에게 유일한 ID 할당, 접근통제 정책 마련, 접근통제 절차 이행, 비상시 접근 절차 수립, 자동 로그오프, 접근 종료
감사통제	N/A
무결성	개인의료정보 인증을 위한 메커니즘 실행
인증	N/A
전송보안	무결성 통제 실행
네트워크 통제	N/A

4.5 조직 요구사항

조직 요구사항은 의료정보취급기관과 사업 파트너 간의 양해각서를 포함한 계약서 및 기타 협정에 관련된 요구사항을 그 내용으로 한다.

사업 파트너의 개인의료정보보호 의무 명시 조항, 사업 파트너 대리인의 개인의료정보보호 의무 명시 관련 사항, 사업 파트너의 보안사고 보고 의무 명시 및 계약 파기 조건 명시 조항이 핵심활동으로 포함되어 있다. 네 가지 활동 모두 필수 사항으로 모든 의료정보취급기관이 반드시 준수해야 한다.

4.6 정책 및 절차 문서화

정책 및 절차 문서화는 보안표준에서 요구하고 있는 정책, 절차, 행동, 활동, 평가를 문서화해서 보관하여 책임자가 사용 가능하도록 해야 하며, 필요 시 갱신해야 한다는 점을 규정하고 있다.

보안규정의 상세이행지침과 표준, 다른 요구사항을 준수하는 논리적이고 적합한 정책과 절차를 이행해야 하며, 문서화된 정책과 절차를 주기적으로 평가해야 한다. 이는 정책과 절차가 보안규정의 표준, 상세이행지침, 다른 요구사항을 충분히 반영해야 한다는 점과 정책과 절차가 부서, 직원, 시스템, 사업 파트너에 의해 나타나는 실제 활동을 정확히 반영해야 한다는 점을 보장해 주기 위한 것이다. 또한 정보보호 관련 정책과 절차는 필요 시 적절하게 변경되어야 한다. 변경사항은 반드시 보안규정의 요구사항에 따라 문서화해야 한다.

보안을 강화하기 위한 보안 규정의 문서화 의무와 문서 보관 의무, 문서 가용성 보장, 주기적 문서 업데이트 의무도 이 영역에 포함된다. 이 가운데, 문서 보관과 문서 가용성 보장은 필수적인 핵심활동으로 분류된다.

5. 의료정보보호 표준 개발의 의의

본 장에서는 본 연구에서 개발한 의료정보보호 표준의 의의 및 중요성을 제시하였으며, 특히 본 연구가 기존 연구들에 비해 갖는 차별성을 기술하였다.

전자의무기록 도입 확대와 e-Health 및 u-Health 확산 등으로

인해 의료정보의 데이터베이스화 및 네트워크를 통한 정보의 교류 및 활용도가 높아지고 있다. 의료정보화 발전과 함께 소비자 중심주의 및 소비자 보호운동의 시대 도래로 환자의 알 권리 보장 및 사생활 보호를 위한 철저한 건강정보보호 대책이 요구되고 있다. 또한 기존의 치료위주의 서비스에서 예방/건강 증진 등의 삶의 질에 중심을 둔 포괄적 보건의료 서비스 제공에 대한 욕구가 커지고 있다. 이러한 배경에서 보건복지부에서는 환자의 개인의료정보 보호를 위한 법 제정 작업을 진행 중이다.

'건강정보보호 및 관리·운영에 관한 법률'이란 명칭의 이 법안에는 건강기록의 열람 및 정정, 건강기록의 교류, 건강기록의 제공·수집에 대한 보호조치, 동의 철회권, 통계·연구목적 등에 대한 보호조치, 건강정보보호위원회의 설치 및 기능, 건강기록의 보호조치, 건강정보보호 수준평가 등을 주요 골자로 포함하고 있다.

특히 이 법안에 포함된 건강기록의 보호조치 관련 조항에는 '보건복지부장관은 관리적·물리적·기술적 조치가 포함된 건강기록 보호지침을 고시할 수 있으며, 생성기관 및 취급기관은 이를 준수하여야 함'을 명시하고 있다.

본 연구의 의의는 바로 이러한 점에서 찾을 수 있다. 즉, 의료정보보호 관련 법안 제정이 가시화 되고 있는데, 이 법안에 명시하고 있는 정보보호 대책을 뒷받침할 수 있는 표준안을 본 연구에서 제시함으로써 국가 차원의 의료정보보호 수준 제고에 기여하고 있다.

본 논문에서 제시한 정보보호 표준안은 보건복지부에서 운영하고 있는 의료정보표준화 위원회 산하의 공식 정보보호 위원회와 건강정보보호 자문위원회 등에서 의료계 전문가, 정보보호 전문가 등이 참여하여 개발된 것으로 향후 의료정보보호 관련 법안이 제정되고 나면 후속조치로 표준안의 공식 제정으로 이어질 것으로 전망된다.

본 연구는 기존의 관련 연구 및 노력들과는 다음과 같은 점에서 차별화된다.

첫째, 기존 연구들은 의료정보 보호에만 초점을 맞추어 규제 위주로 추진된 데 비해 본 연구는 의료정보 보호와 의료정보취급기관의 업무 효율을 함께 고려하여 현장 활용 가능성을 크게 높였다. 표준 개발 과정에 의료정보시스템 구축 및 운영 전문가와 의료정보 관리자들이 직접 참여하였으므로 의료 현장에 적용할 때 시행착오를 최소화할 수 있을 것으로 기대된다.

둘째, 기존의 연구 및 관련 노력들은 소수 연구자에 의해 추진되었으나 본 연구에서는 각 영역의 전문가들로 구성된 분과위원회를 구성하여 표준안을 개발함으로써 각 영역 내에서의 검증을 거쳤다. 물론 추후에 관련법이 통과되고 나면 한 차례 더 의견 수렴 및 수정보완 작업이 이루어져야 할 것이다.

셋째, 기존의 연구들이 실제 의료 현장에 적용되지 못하고 연구 수준에서 머무른 데 비해 본 연구에서는 정부의 적극적인 정책의지를 바탕으로 실제 의료기관들이 정보 보호에 활용하는 것을 전제로 표준안을 개발하였다.

정보보호는 일시적인 노력으로 해결되는 것은 아니다. 신규 자산 및 정보시스템의 확충, 새로운 위협 및 취약성의 증가 등으로 인해 새로운 보안 위험은 나타나기 마련이다. 따라서 지속적인 정보보호 관리 체계를 갖출 필요가 있다. 본 연구에서 제시한 의료정보보호 표준은 의료정보취급기관이 지속적인 정보보호 관리 체계를 확립하는데 있어 참조할 수 있는 기준이 된다.

6. 결론 및 추후 연구과제

여타 산업과 마찬가지로 의료 분야 또한 e-비즈니스가 고도화됨에 따라 유비쿼터스 건강관리 서비스, 개인 맞춤형 건강관리, 평생 전자건강기록(EHR), 국가보건의료정보인프라(NHII) 구축 등의 영역에서 의료정보의 데이터베이스화 및 네트워크를 통한 공유 및 활용성 제고에 대한 요구가 커지고 있다. u-Health로 표현되는 유비쿼터스 사회에서의 개인 건강관리 서비스 시대에 대비하기 위해서는 개인의료 정보를 생성, 저장, 관리, 활용하는 기관들의 의료정보보호 수준 제고가 반드시 선행되어야 한다.

국내 관련 부처에서도 환자의 개인의료정보 보호를 위한 법률 제정을 추진 중이다. 이 법안에 포함된 의료정보취급기관의 의무인 정보보호 대책의 세밀한 규정의 제정 작업은 의료정보보호 수준을 제고하기 위해 반드시 수행되어야 한다.

본 연구에서 개발한 의료정보보호 표준에는 10개의 세부항목으로 구성된 관리적 정보보호 방안, 5개의 세부항목으로 구성된 물리적 정보보호 방안, 6개의 기술적 정보보호 방안, 그 외 조직요구사항, 정책 및 절차 문서화 관련 세부 항목이 각각 1개, 2개가 포함되어 있다. 본 연구에서 제시한 정보보호 표준안은 구체적 기술을 명시하는 방식 보다는 보안 요구사항을 해결하기 위한 포괄적이고 중립적인 정책, 절차, 기술을 규정하고 있다.

본 연구에서는 실제 의료 현장에서 정보 보호에 활용하는 것을 전제로 표준안을 개발하였다. 본 연구의 결과는 보안업체 전문가, 의료기관 정보보호 담당자, 의사, 정보관리자, 학계 전문가 등 각 영역의 전문가들로 구성된 분과위원회에서 검증을 거쳤다.

본 연구에서 제시한 의료정보보호 표준안은 향후 관련분야 전문가, 의료 분야 이해관계자들의 검토를 거쳐 국가 차원의 표준으로 제정될 것으로 예상된다. 본 연구에서 개발한 의료정보보호 표준안을 활용하여 의료정보취급기관들은 종합적인 정보보호 체계를 갖추고 환자의 프라이버시 보호 수준을 한층 강화할 수 있을 것이다. 또한 의료기관간 정보 공유 체계 구축 등 국가차원의 의료정보 인프라 구축과 u-Health 환경의 도래로 인해 제기되고 있는 개인의료정보보호에 대한 우려를 불식시키는데 기여할 것으로 기대된다.

일단 표준이 제정되어 보급되고 나면 의료기관이 보안 표준을 얼마나 준수하는지 평가하고 인증하기 위한 체계가 필요하

다. 따라서 표준안 제정 이후에는 보안 표준에 대한 인증 체계에 대한 연구가 필요하다. 국외 사례와 국내 타 분야의 사례를 참조하여 최적의 방안을 모색할 필요가 있다.

보안 표준의 준수가 의료기관의 일방적인 부담으로만 작용해서는 곤란하며, 의료기관이 개인정보보호 규정 및 보안 표준을 잘 따르면서 효율적인 정보 이용과 정보보호를 동시에 달성할 수 있도록 제반 여건을 조성해야 한다.

의료기관이 본 연구에서 제시한 정보보호 표준 규정에서 정의하고 있는 사항을 충족시키기 위해서는 추가적인 비용과 노력이 필요하다. 이러한 비용과 노력은 정보화를 통한 효율성 제고와 환자 개인의료정보의 보호라는 두 가지 목표를 충족시키기 위해 지불해야 하는 비용이라 할 수 있다.

의료정보 취급기관들은 본 연구에서 제안한 표준을 준수하여 개인의료정보보호수준을 향상시키기 위해 전사적 정보보호 아키텍처를 갖출 필요가 있다. 정보보호 정책 및 정보보호 관리 절차 및 규정, 조직 체계를 확보하고 정보보호 아키텍처 전반에 걸쳐 체계성을 확보하여 정보보호 기반을 마련해야 한다. 조직의 모든 구성원들이 정보보호에 대한 인식을 전환할 수 있도록 교육과 훈련을 실시하는 등 정보보호 문화의 확산을 위한 노력이 필요하다.

참고문헌

Ahern, D. K., Kreslake, J. M., and Phalen, J. M. (2006), What Is eHealth (6): Perspectives on the Evolution of eHealth Research, *Journal of Medical Internet Research*, **8**(1).

Chae, Y-M. (2005), *Establishing Laws and Regulations for e-Health Promotion*, Project Report of MOHW, Seoul, Korea.

Efraim Turban and David King (2003), *Introduction to e-Commerce*, Prentice Hall, New Jersey.

Eng, T. R. (2001), *The eHealth Landscape, A terrain map of emerging information and communication technologies in health and health care*, Princeton, NJ: The Robert Wood Johnson Foundation.

Eysenbach, G. (2001), What is e-health?, *Journal of Medical Internet Research*, **3**(2).

Jim, Moynihan, The Basics of Healthcare EDI/EC, HIPAA Summit West II, March 14, 2002. Available at www.ehcca.com/presentations/ HIPAAWest2/ 1_01.pdf.

Joan, Hash *et al*. (2005), *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act(HIPAA) Security Rule*, NIST Special Publication 800-66.

KHIDI (2004), *Privacy and Security Standard for Electronic Medical Record*, Research Report, Seoul, Korea.

Kim, D. and Kim, M. (2006), Issues on Privacy and Security of Health Information in u-Health IT Service Environment, *Proc. 2006 Spring Conf. of Korea Society of IT Services*, 282-289.

Kim, D. and Park, H. (2003), A Review of Hospital Information Systems and e-Hospital Strategy Development of Large-sized Hospitals, *Informatization Policy*, **11**(3), 13-29.

Kim, T-J. and Kim, I-H. (2005), A Study on Individual Information Security Management System in Ubiquitous Environment, *Security News*, 10-15.

MOHW (2006), *A Study on Health Information Security Standard*, Project Report of MOHW, Seoul, Korea.

Oh, H., Rizo, C., Enkin, M., Jadad, A., Powell, J., and Pagliari, C. (2005), What Is eHealth (3): A Systematic Review of Published Definitions, *Journal of Medical Internet Research*, **7**(1).

P&AB and Harris Interactive, Available at http://www.pandab.org/ healthpr. html.

Pagliari, C., Sloan, D., Gregor, P., Sullivan, F., Detmer, D., Kahan, J. P., Oortwijn, W., MacGillivray, S., and Griffiths, F. (2005), What Is eHealth (4): A Scoping Exercise to Map the Field. *Medical Internet Research*, **7**(1).

United States Department of Health Human Service, *Standards for Privacy of Individually Identifiable Health Information, Security Stands for the Protected Health Information, General Administrative Requirements Including, Civil Money Penalties, Regulation Test(45 CFR Parts 160 and 164)*.

김 동 수

서울대학교 산업공학과 학사
서울대학교 산업공학과 석사
서울대학교 산업공학과 박사
현재: 숭실대학교 산업・정보시스템공학과 조교수
관심분야: BPM, u-business, SOA, u-Health, 정보보호

김 민 수

서울대학교 산업공학과 학사
서울대학교 산업공학과 석사
서울대학교 산업공학과 박사
현재: 부경대학교 시스템경영공학과 조교수
관심분야: BPM, RosettaNet, eAI, 의료정보보호, 물류 프로세스 관리