HEALTHCARE POLICY
pISSN 1975-8456 / eISSN 2093-5951
J Korean Med Assoc 2015 December; 58(12): 1159-1170
http://dx.doi.org/10.5124/jkma.2015.58.12.1159

한국형 원격의료체계 기술적 안전성 평가체계 수립에 대한 연구

이 희 주[1] · 남 초 이[1] · 윤 장 호[1] · 윤 준 섭[1] · 이 호 진[1] · 김 진 숙[2] · 김 석 영[2] · 최 재 욱[2-4] · 이 경 호[1] | [1]고려대학교 정보보호대학원, [2]대한의사협회 의료정책연구소, 고려대학교 [3]의과대학 예방의학교실, [4]환경의학연구소

A study on establishing a technical safety assessment system for the Korean telemedicine system

Hee Joo Lee, MS[1] · Choi Nam, MS[1] · Jang Ho Yun, MS[1] · Jun Seob Yoon, MS[1] · Ho Jin Lee, MS[1] · Jin Suk Kim, PhD[2] · Seok Yeong Kim, MBA[2] · Jae Wook Choi, MD[2-4] · Kyung Ho Lee, PhD[1]

[1]Graduate School of Information Security, Korea University, Seoul; [2]Research Institute for Healthcare Policy, Korean Medical Association, Seoul; [3]Department of Preventive Medicine, Korea University College of Medicine, Seoul; [4]Institute for Occupational and Environmental Health, Korea University, Seoul, Korea

Telemedicine is a critical infrastructure that directly affects people's lives. In this vein, the government announcement of the introduction of a telemedicine service has caused controversy among the government and medical institutions over the safety of the service. Before the introduction of the telemedicine service, its technical safety and effectiveness should be validated. The telemedicine system should be supported by proper policies to ensure a secure, continuous service. To this end, we have conducted research to derive the security requirements from domestic and foreign standards and laws relating to telemedicine and information security. Based on the derived requirements, we have developed a security standard for telemedicine that facilitates the objective assessment of the security of the telemedicine service. Furthermore, we have analyzed the vulnerabilities of telemedicine devices through penetration tests. Finally, using a risk analysis method, we have created risk scenarios that might occur in the provision of telemedicine services, and have calculated risk levels and expected loss for each scenario. We expect that the results of this research will be a basis for ensuring a sufficient budget and staff for the safety of telemedicine, and for establishing relevant policies.

Key Words: Telemedicine; Technical safety assessment; Risk analysis; FAIR methodology

서론

2015년 5월 한국 사회는 중동호흡기증후군(Middle East respiratory syndrome, MERS; 메르스)라는 호흡기감염증 환자가 증가함에 따라 사회적 혼란을 겪었다. 병원 내에서 치료를 받고 있던 보균환자들에 의해 병원 이용 환자들 간 메르스균이 급속하게 전파됨에 따라 정부는 일부 병원에 원격의료서비스를 허용하는 지침을 발표하였다. 이 지침을 통해서 감염 진원지 병원은 의료인이 전화로 환자를 진료하고 의약품을 처방하는 원격진료를 한시적으로 허용되었다. 이는 기존의 대면진료를 통해 의료인이 환자를 직접 진료하여 치료를 하던 절차와는 달리, 비 대면으로 원격지에서 환자를 진료하는 원격의료서비스의 일부를 실시한 것이다. 이에 따라, 원격의료서비스의 기술적 안전성이나 치료의 효과성 등의 우려가 커짐에 따라 원격의료를 둘러

Received: September 9, 2015 **Accepted:** October 16, 2015

Corresponding author: Kyung Ho Lee
E-mail: kevinlee@korea.ac.kr

싼 국민적 관심이 어느 때보다 높아지고 있다[1].

2000년 초반, 정부는 의료법 개정 이후 시스템 구축을 통한 단순 진료위주의 시범사업에서 탈피하여 정부 주도 공공의료서비스 중심의 서비스 모델 사업들을 본격적으로 추진하였다. 정부에서는 원격의료산업 활성화 촉진 및 고령화 사회에 대한 대책을 마련하기 위해 2006년부터 다양한 원격의료시범사업을 추진하고 있다. 의료취약계층 해소, 의료복지 수준향상, 사회적 편익 및 안전망 확충 등 사용자 중심의 공공의료서비스 제공을 위해 다양한 원격의료 서비스 모델을 개발 및 적용하였다[2]. 2009년 이후에는 원격의료 관련 기술, 콘텐츠 개발, 인력약성 등의 사업을 추진하였다.

정부는 본격적인 원격의료 도입을 위해 2014년 9월말부터 의사–환자 간 원격의료에 대한 1단계 시범사업을 진행하였고, 현재는 2단계 시범사업이 추진되고 있다[3]. 하지만 의료분야의 전문단체들은 원격의료사업의 검증되지 않은 안전성을 우려하며 원격의료에 대해 반대의사를 표시하고 있다. 이와 같이 정부와 의료 분야 전문기관의 원격의료를 둘러싼 논쟁으로 완벽한 원격의료서비스의 도입은 아직 이루어지지 않은 상태이다[4].

원격의료는 국민의 생명을 담보로 하는 국가의 중요 인프라 중에 하나이다. 그럼에도 불구하고 아직까지 기술적 안전성에 대한 기준 수립 및 검증이 미흡한 상태이다. 원격의료서비스에서 취급하는 정보는 유출 시에 환자 개인의 사회생활을 위협할 뿐만 아니라, 의료기관에도 금전적 손실을 가져다 줄 수 있다. 또한, 해킹으로 인한 의료정보의 변조 및 손실로 인하여 환자의 생명에 치명적인 문제가 발생할 수 있다.

원격의료서비스가 선진화 된 미국에서는 의료정보유출과 같은 원격의료의 위험성을 인식하고, 이에 따라 안전성을 보장하기 위하여 각종 조치를 취하고 있다[5]. 반면에 국내에서는 원격의료에 대한 위험성이 과소평가 되어 적절한 조치가 이루어지지 않고 있다. 또한, 정책적 지원이 미흡하여 원격의료서비스 중 의료정보유출 및 의료사고 등이 발생할 경우 책임 소재 규정의 문제 등 법 · 제도적 문제점이 존재한다.

원격의료를 진행하기 위해서는 원격의료의 기술적 안전성과 개인의 건강정보보호 그리고 원격의료의 비용효과성 등을 고려하여야 한다. 정부에서는 1차 원격의료시범사업의 결과로 긍정적인 평가를 내놓았지만 의료계에서 가장 우려하는 원격의료의 기술적 안전성과 유효성에 대해서는 검증결과를 공개하지 않은 상태이다[6]. 이러한 쟁점들을 판단할 수 있는 공개적이고 객관적인 검증은 원격의료 허용 전 우선적으로 해결되어야 할 과제이다.

원격의료는 환자와 의사가 의료기관 외부에서 통신수단을 활용하여 의료 정보 및 처방 정보들을 교환해야 한다. 이때, 개인정보를 포함한 질병 · 처방 · 건강정보 등이 정보유출의 위험에 노출될 수 있다. 인터넷이 활성화 되면서 개인정보 유출이 심각한 문제가 되고 있는데 건강정보가 유출되고 악용된다면 그 사회적 파급효과와 피해자가 입을 손해는 막대할 것이다. 정부는 원격의료 허용과 동시에 정보보호 규정강화 및 관리 · 감독 체계 신설 등 추진계획을 마련하겠다고 하였으나 현재 시행되고 있는 시범사업의 시스템에서도 취약점들이 발견된 상태이다[7].

본 연구는 한국형 원격의료체계의 기술적 안전성 평가체계 수립을 목표로 한다. 원격의료 안전성 평가 영역에는 기술적, 임상적, 환경적인 부분이 포함된다. 그 중 기술적 안전성이란, 의료 기기의 기술적 장애, 정보보호 사고, 해킹 등을 통한 개인정보의 유출 및 변조, 의료시스템의 운영 중단 등이 발생할 수 있는 부분을 보호하는 것을 의미한다. 특히 원격의료의 기술적 안전성이란, 환자와 의료인간 원격진료가 진행 될 때 주고받는 개인정보 및 의료정보가 대면진료에 준하는 정보의 기밀성, 무결성, 가용성을 보장하는 것을 말한다. 기밀성이란 암호나 패스워드 같이 인가된 사용자만 자산에 접근할 수 있는 것을 말한다. 무결성이란 적절한 권한을 가진 사용자만이 인가된 방법으로만 정보를 변경할 수 있는 것이고, 가용성이란 적절한 시간에 자산에 접근이 가능한 것을 의미한다.

국제 정보보호 관리체계인 IEC/ISO 27001 [8]의 구조를 보면 통제를 구현하기 위해 체크리스트 형태로 구성된 Gap 분석과 자산을 선별하고 자산에 대한 위협 및 위험을 분석하는 위험분석이 있다. 이 두 개의 분석을 모두 포함한 것을 정보보호 관리체계라 일컫는다. 본 연구는 원격의료의 기술적 안전성 평가체계 수립을 위해 먼저 국내 · 외 정보보호 및

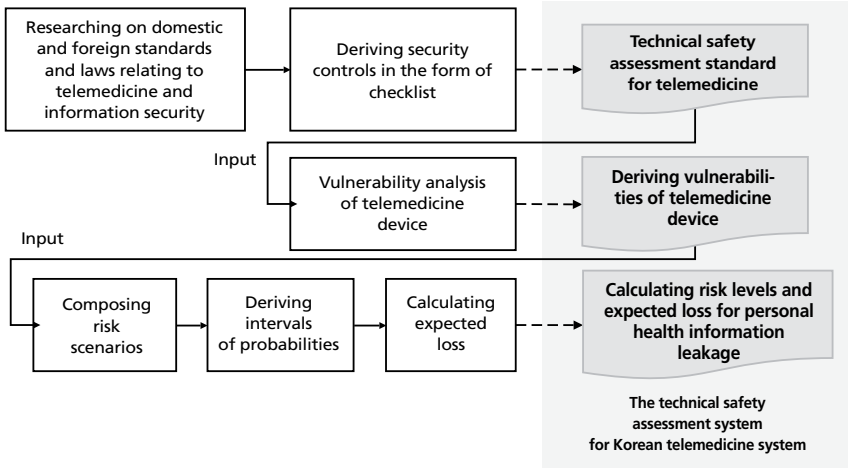

Figure 1. Composing of the technical safety assessment system for Korean telemedicine system.

Table 1. Comparison of IEC/ISO 27001 for information security management systems and the technical safety assessment system for Korean telemedicine system

IEC/ISO 27001 for information security management systems	The technical safety assessment system for Korean telemedicine system
Gap analysis	Technical safety assessment standard for telemedicine
Risk analysis	Deriving vulnerabilities of telemedicine device
	Risk analysis process using factor analysis of information risk method

원격의료체계의 표준 및 법령을 비교분석하여 체크리스트 형태의 '원격의료체계 기술적 안전성 평가기준'을 개발한다. 그리고 개인의 건강정보 유출사고 시 발생할 수 있는 피해 규모를 도출하기 위해 factor analysis of information risk (FAIR) 방법론[9]을 통하여 위험분석을 수행한다. 한국형 원격의료체계의 기술적 안전성 평가체계의 구성은 Figure 1과 같다. 또한, IEC/ISO 27001의 정보보호 관리체계 구성과 본 연구팀이 제시하는 한국형 원격의료체계의 기술적 안전성 평가체계의 비교는 Table 1과 같다.

한국형 평가체계를 수립하기 위해서는 다음을 이해해야 한다. 첫째, 해외 병원과의 교류 및 진출 등과 같은 시장의 확대 기회를 위해 세계적 기준을 수용해야 한다. 둘째, 정책결정자의 의사결정에 도움을 주고자 superset을 만들어 완벽한 틀을 제공해야 한다. 마지막으로 의료사고 발생 시, 법정에서 민 · 형사적인 기준이 될 수 있는 명확한 기준을 제시할 수 있어야 한다.

연구내용 및 방법

1. 원격의료체계 기술적 안전성 평가기준

원격의료체계 기술적 안전성 평가기준을 개발하기 위한 단계로 Figure 2와 같은 프로세스를 진행한다.

1) 정보보호 및 원격의료체계의 국내 · 외 표준 및 법령 조사

본 연구는 원격의료체계의 기술적 안전성을 평가 할 수 있는 기준을 개발하기에 앞서 정보보호체계와 원격의료체계의 국내 · 외의 표준 및 법령을 조사하였다. 국내의 표준 및 법령에는 조직의 정보보호 관리체계에 관한 Korea Information Security Management System (K-ISMS) [10], 개인정보의 보호를 법적으로 명시한 개인정보보호법[11], 정보통신망 이용촉진 및 정보보호 등에 관한 법률[12] 그리고 국민 의료에 관한 사항을 규정한 의료법[13] 등을 조사하였다. 아직 국내에는 원격의료에 특화된 체계가 부재하여 미국, 호주, 캐나다의 원격의료 체계를 조사 및 분석하였다.

정보보호체계에 대해서는 국제 표준인 ISO/IEC 27001, ISO/IEC27002 [14]와 의료 분야의 정보보호 구현 가이드인 ISO 27799 [15]를 조사하였다. 미국의 의료법인 Health Insurance Portability and Accountability Act (HIPAA) [16]에는 의료 분야에서 기술적 안전성을 유지하기 위한 법조항을 포함하고 있다. 또한, 이를 구현하기 위해 발표된 NIST SP 800-66 [17] 구현가이드를 조사하였다.

2) 체크리스트 형태의 통제항목 도출

원격의료체계의 기술적 안전성 평가기준을 개발하기 위하여 조사된 국내 · 외 표준 및 법령을 분류하였다. 표준 및 법령은 크게 4가지로 ISO 국제 표준, 국외 원격의료 관련 가이드라인, 미국의 의료 관련 법령 및 표준, 국내 법령 및 표준으로 구분하여 원격의료 관련 국내 · 외 표준의 관계를 도출하였다. 관계를 도출한 4가지 구분의 상세 내용은 Table 2 [18-24]와 같다.

도출된 내용을 바탕으로 원격의료 서비스의 안전성을 평가

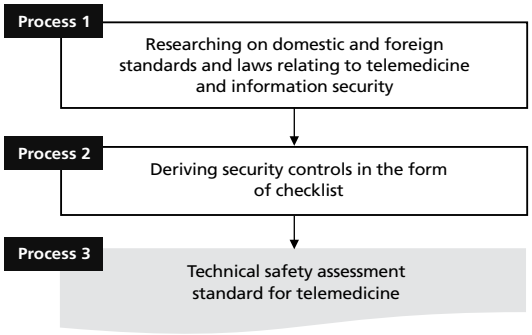

Figure 2. A process to develop technical safety assessment standard for telemedicine.

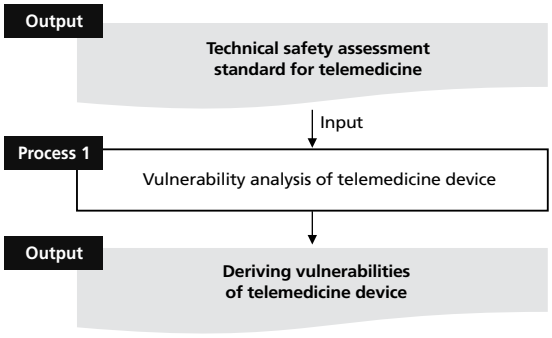

Figure 3. A process to analyze vulnerabilities of telemedicine device.

Table 2. Categorization of standards and laws

Category	Law and standard
ISO International standard	ISO/IEC 27001, ISO/IEC 27002, ISO 27799, ISO/TS 13131 [18]
Telemedicine guideline by foreign	ACRRM TeleHealth Advisory Committee Standards Framework [19], Practice Guidelines for Video-Based online Mental Health Service [20], Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions [21], Good Medical Practice: A Code of Conduct of Doctors in Australia [22], ISO/TS 13131
The laws and standards relating to healthcare in the US	HIPAA, NIST 800-66
The laws and standards in Korea	K-ISMS, Medical Service Act, Personal Information Protection Act, The standard for security measure of personal information [23], Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., The standard for physical/technological/administrative measures [24]

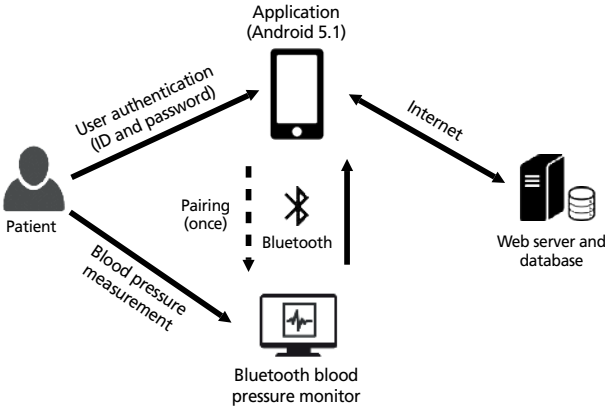

Figure 4. Vulnerability analysis diagram of telemedicine device.

할 수 있는 '원격의료 분야'와 의료분야 전체를 평가할 수 있는 '의료 분야'로 나누어 평가기준을 개발하였다. 평가기준은 체크리스트 형태의 총 195개의 통제 항목으로 구성하였다.

2. 원격의료 기기 취약점 분석

원격의료에서 사용되고 있는 기기들의 보안 위험을 확인하기 위해 취약점 분석을 실시하였다. 취약점 분석이란, 식별된 자산이 근본적으로 가지고 있는 약점을 찾아내는 과정이다. 일반적으로 자산의 기밀성, 무결성, 가용성 등에 영향을 미칠 수 있는 다양한 위협에 대해 자산의 취약점을 인식하고, 이로 인해서 예상되는 손실 및 결과를 분석하는 것을 말한다.

본 연구에서 진행하는 취약점 분석은 기기의 기술적 취약점을 확인하는 것으로 개인정보와 인증정보가 전송되는 구간에서 얼마나 취약한지를 확인하고자 하였다. 원격의료체계 기술적 안전성 평가기준의 결과를 취약점 분석 시 이용한다. 예를 들어 원격의료기기나 의료시스템의 취약점을 분석하기 위해서는 평가기준의 결과를 바탕으로 Figure 3과 같이 분석을 진행한다.

취약점 분석에 대상이 된 원격의료기기는 블루투스 통신기능을 이용하여 혈압을 측정하는 기기로 지정하였다. 이 기기는 의료-환자 간 원격 자가 건강관리 사업에서 사용하는 실제 기기이다. 실제 사용 환경에서의 취약점을 측정하기 위해 Figure 4와 같이 통신구간을 나누어서 취약점을 분석 하였다. 첫 번째 통신구간은 혈압계와 스마트기기간의 통신구간으로 구분하였다. 두 번째 통신구간은 스마트기기와 서버간의 통신구간으로 구분하여 각 구간의 취약점 분석을 실시하였다.

3. 위험분석을 통한 피해규모 산정

유출사고의 피해규모를 도출하기 위해 위험분석을 Figure 5와 같이 진행하였다. 위험분석은 FAIR 방법론을 사용하였다. FAIR 방법론은 최근에 선진기업에서 많이 사용되는 방

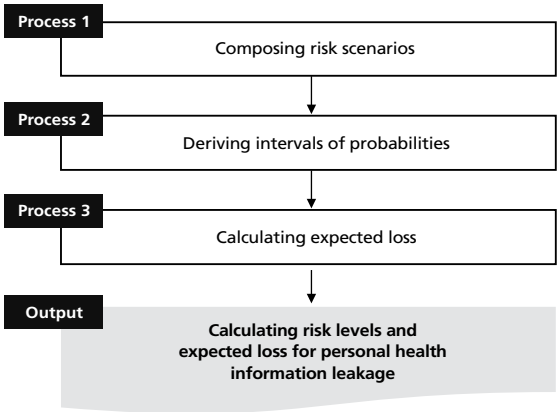

Figure 5. Vulnerability analysis diagram of telemedicine device.

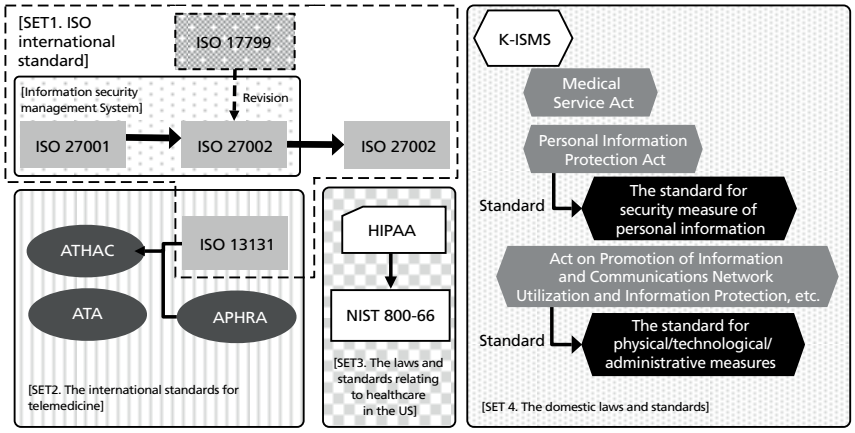

Figure 6. The relationship between domestic and international standards relating to information security and telemedicine. ATHAC, Austrian College of Rural & Remote Medicine Telehealth Advisory Committee; ATA, American Telemedicine Association; APHRA, Australian Health Practitioner Regulation Agency; HIPAA, Health insurance Portability and Accountability Act.

법론으로 사이버 상에서의 보안 및 운영의 위험 값을 측정하는 국제모델이다. 이 방법론을 통해 정성적으로 위험을 분석할 뿐만 아니라 정량적으로도 위험을 분석하여 피해규모 산정이 가능하다. FAIR 방법론은 시나리오를 기반으로 위험의 정량적인 값을 산출하는 위험분석 방법 중 하나이다.

FAIR 방법론으로 도출된 위험의 신뢰도는 다음 두 가지 요소로 평가된다. 첫 번째, FAIR 방법론에서 사용되는 위험 시나리오의 현실가능성이다. 위험 시나리오는 위험자산, 위협원, 조직의 특성 등이 반영된 시나리오를 의미한다. 따라서 현실가능성이 존재하지 않는 시나리오는 아무리 위험이 높다 하더라도 고려되지 않는다. 본 논문에서는 실제 국내에서 일어난 의료개인정보 유출사고와 원격의료기기의 취약점 분석을 통하여 현실가능성이 매우 높은 시나리오를 사용하였다.

두 번째, FAIR 방법론에서 사용하는 사고금액의 적합성이다. 가장 적합성이 높은 금액은 조직이 보유하고 있는 과거의 발생했던 비용을 바탕으로 재 산정된 금액이다. 그러나 본 연구에서는 아직 원격의료가 국내에 활성화 되지 않은 점을 고려하여 미국의 Ponemon 연구소에서 발간한 '2011 Cost of Data Breach Study: United States' 보고서[25]에 제시되고 있는 health 분야 피해금액을 사용하였다. 이 보고서는 미국뿐만 아니라 영국, 독일, 오스트레일리아, 프랑스를 조사대상으로 삼고 있으며 이는 대부분의 국가 및 연구들이 가장 근간이 되는 데이터로 사용하고 있다[26].

연구결과

1. 원격의료체계 기술적 안전성 평가기준 개발

1) 국내 · 외 표준 및 법령의 분류 및 관계 도출

평가기준을 개발하기 위해 조사한 국내 · 외 법령 및 표준을 분석하여 크게 4가지로 분류하였다(Table 2). 각각 연관성 있는 표준들로 분류하여 각 법령 및 표준들의 관계를 도출하였다. 도출한 관계는 Figure 6과 같다.

국제 정보보호 관리체계의 표준인 IEC/ISO 27001의 구현 가이드인 IEC/ISO 27002와 의료 분야의 특성을 고려하여 보안요구사항을 구현하기 위한 가이드인 ISO 27799 등을 포함하여 '구분 1. ISO 국제표준'으로 도출하였다. 이 구분은 조직이 자산을 안전하게 보호하기 위한 보안 요구사항들에 대한 표준들로 향후 의료 분야 통제항목 도출 시 참고하였다.

'구분 2. 국외 원격의료 관련 가이드라인'은 원격의료서비스의 품질향상 및 안전한 운영을 위한 표준 및 프레임워크의 집합이다. 호주 원격의료에 특화된 Austrian College of Rural & Remote Medicine Telehealth Advisory Committee (ATHAC)의 표준과 미국 원격의료에 특화된 American Telemedicine Association (ATA)의 표준 그리

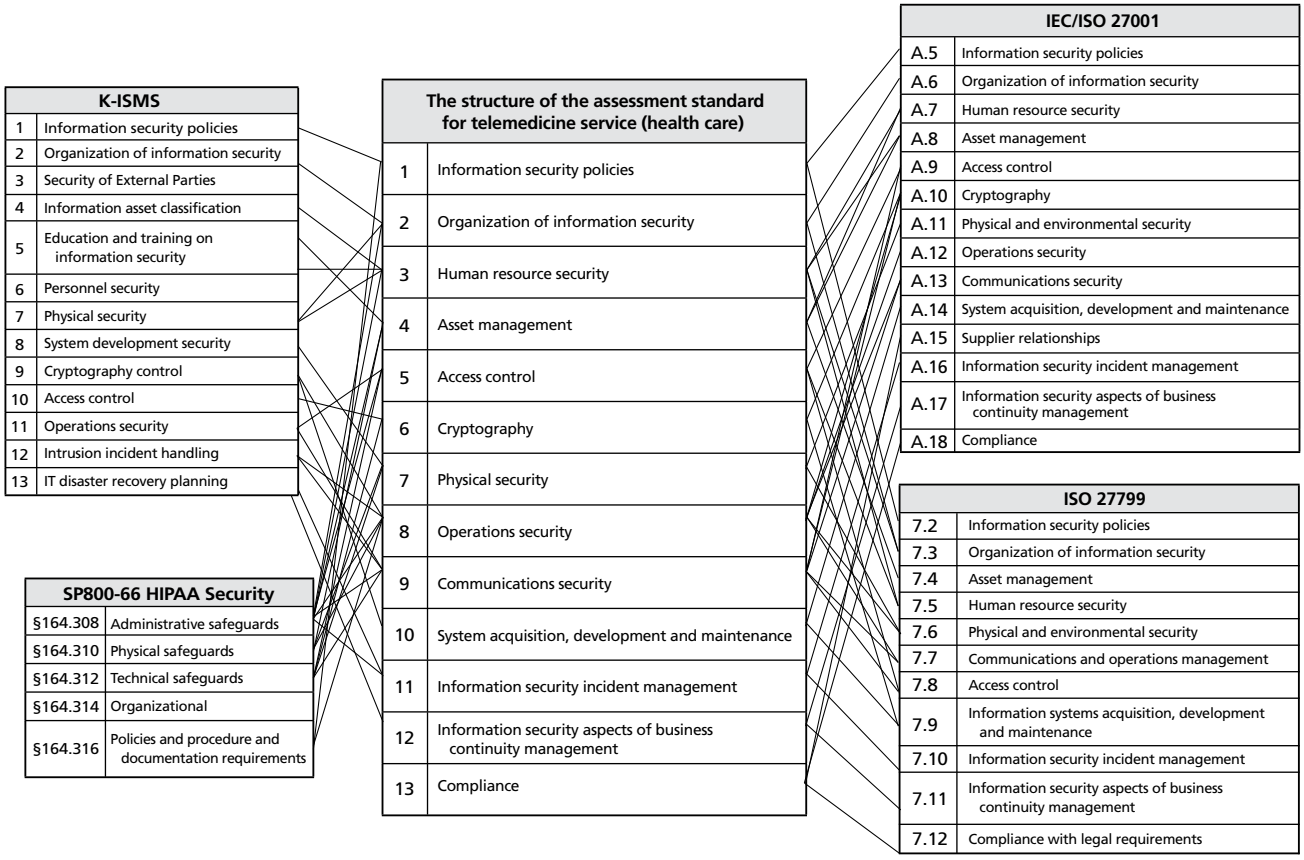

Figure 7. The mapping for healthcare field for assessment standard.

고 의료인이 전반적으로 준수해야 하는 행동규범을 제시하기 위한 호주 Australian Health Practitioner Regulation Agency (APHRA)의 가이드라인이 포함된다. 이 구분은 향후 원격의료 분야의 통제항목 개발 시 참고 하였다.

'구분 3. 미국의 의료 관련 법령 및 표준'은 HIPAA와 NIST 800-66이 포함한다. HIPAA의 법 조항 중 건강정보 및 의료정보에 대한 보안 요구사항을 기술한 HIPAA Security Rule을 참조하였다.

'구분 4. 국내 법령 및 표준'은 국내의 K-ISMS와 개인정보보호법, 의료법, 정보통신망 법과 같은 국내 법령을 참고하였다. 통제항목 형식으로 구성된 K-ISMS은 '구분 1'과 함께 평가기준 개발에 사용되었다. 또한, 국내 법령과 기준들은 통제항목의 세부설명에 자세히 서술하여 사용자의 이해를 돕기 위해 참고하였다.

2) 평가기준 개발

평가기준은 원격의료를 포함한 의료 분야 전체를 평가 할 수 있도록 '의료 분야'와 '원격의료 분야'로 분류하여 개발하였다.

의료 분야에는 의료기관이나 보건소 등 전체적으로 적용할 수 있는 정보보호 정책, 조직, 운영 보안 등과 같은 일반적인 내용을 확인할 수 있다. 의료분 야는 IEC/ISO 27001, K-ISMS, ISO 27799, SP 800-66 HIPAA Security를 매핑하여 13개의 도메인과 52개의 세부항목으로 구성하여 개발하였다. 의료의 전반적인 부분을 평가할 수 있도록 최대한 여러 표준을 포함하였다.

원격의료 분야에서는 원격의료의 임상, 기술, 환경과 같은 원격의료 서비스에 대한 안전성을 확인 할 수 있다. 호주의 ATHAC과 APHRA, 미국의 ATA, 국제표준인 ISO/TS 13131을 매핑하여 3개의 도메인과 10개의 세부항목으로 구성하였다.

원격의료뿐만 아니라 의료의 전반적인 부분을 평가 할 수 있는 기준을 개발하기 위해 다양한 표준을 참고하였다. 예를 들어, 원격의료와 의료의 기술적인 부분에 대해서는 중복되지 않도록 나누어 통제항목을 도출하였다. Figures 7, 8과 같이

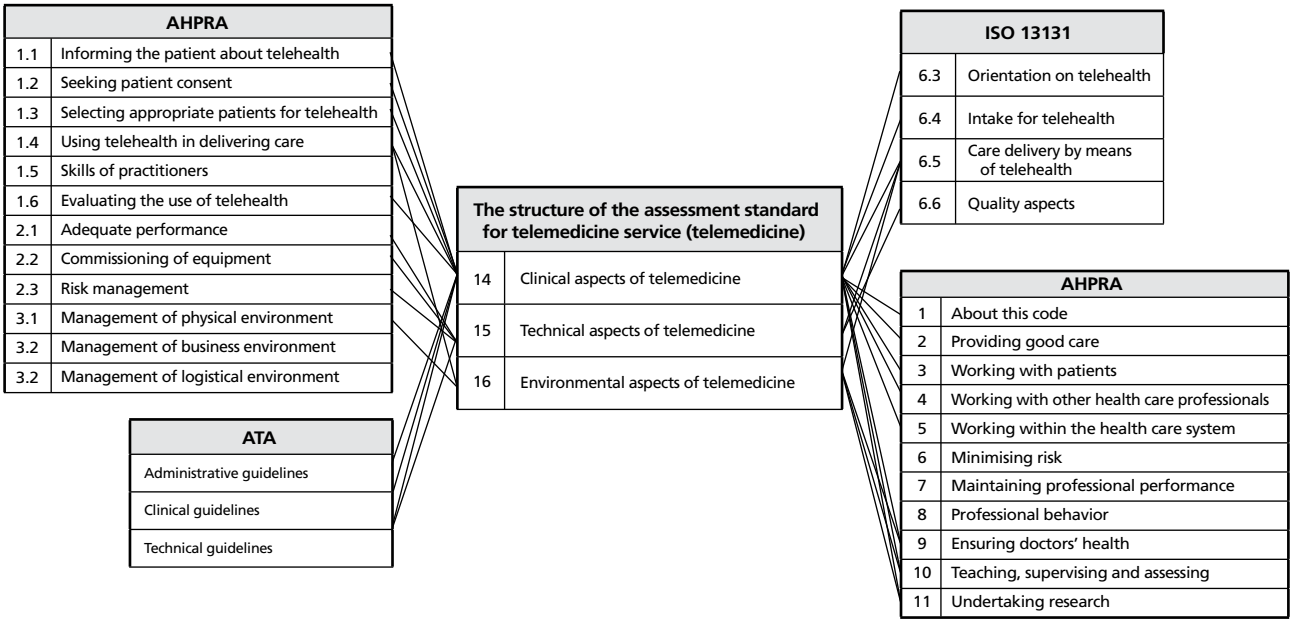

Figure 8. The mapping for telemedicine field for assessment standard.

총 16개의 도메인은 각각의 표준과 가이드라인을 참고하여 매핑하였다. 통제항목은 의료분야 165개와 원격의료 분야 30개로 총 195개를 개발하였다.

2. 원격의료기기의 취약점 도출

개인정보유출 시나리오를 도출하기 위해 원격의료기기의 취약점을 분석하였다. 분석은 원격의료기기, 어플리케이션이 설치되어있는 스마트기기(이하 스마트기기), 서버 구간으로 나누어 분석하였다. 원격의료기기에서 사용되는 정보는 개인을 식별 및 인증하기 위한 인증정보와 의료서비스를 위한 개인건강정보를 포함한 개인정보로 구분된다.

원격의료기기의 취약점을 분석한 결과, 의료기기에서 수집 및 처리되는 데이터에 대한 암호화가 이루어지지 않아 모든 정보가 평문으로 전송 및 저장되는 문제점을 도출하였다. 데이터의 암호화는 데이터를 보호하기 위한 가장 기본적인 조치로 이러한 취약점이 발견된 것은 원격의료기기에 보안조치가 거의 되어 있지 않다는 것을 의미할 수 있다. 취약점으로는 크게 비 암호화 통신, 파라미터 변조, 데이터의 비 암호화, 통신상의 인증 취약점이 도출되었다.

1) 스마트기기와 서버 간 데이터가 평문으로 전송되어 개인정보 탈취 가능

스마트기기와 서버 간 전송되는 패킷을 분석한 결과, 개인건강정보와 인증정보를 비롯한 개인정보가 암호화되지 않은 채 전송되는 것을 확인하였다. 본 연구는 패킷 캡쳐 프로그램인 '와이어샤크'를 이용하여 통신에서 전송되는 패킷을 획득하였다.

확인된 취약점은 사용자가 스마트기기에 설치된 프로그램에 로그인 시 전송되는 정보(사용자 아이디와 비밀번호, 생년월일, 키, 체중, 휴대폰번호, 성별, 식별번호 등)의 탈취가 가능하였다. 또한 사용자가 원격의료기기를 사용하여 측정한 결과를 전송하는 패킷을 통해서는 개인의료정보(수축기, 이완기, 맥박, 체중, 운동여부, 복약여부 등)의 탈취가 가능하였다. 해당 취약점을 이용하면 악의적인 공격자는 패킷에 포함된 인증정보나 개인건강정보를 비롯한 각종 개인정보를 탈취할 수 있다.

2) 파라미터 변조를 통한 권한 없는 행위 가능

스마트기기와 서버 간 전송되는 패킷에 대한 보안조치가 부재하여 변조가 가능하였다. 서버는 패킷에 포함된 식별번호 파라미터를 통해 사용자를 식별한다. 그러나 식별번호에 대한 별도의 인증절차가 부재하여 악의적인 공격자가 식별번호 파라미터를 타인의 식별번호로 변조하여 재전송할 경우, 서버는 해당 패킷이 타인으로부터 전송된 것으로 인식하였다. 이

Table 3. Leaked scenario

Area	Risk asset	Threat	Threat type	Threat effect
System area	Medical information (diagnosis and clinical outcome)	Unauthorized employee	Data breach	Confidentiality

를 이용하면 타인의 개인의료정보를 임의로 생성할 수 있다.

또한, 비밀번호를 변경하는 패킷의 식별번호와 비밀번호 파라미터를 변조할 경우, 악의적인 공격자는 임의로 타인 계정의 비밀번호를 변조할 수 있었다. 만약, 악의적인 공격자가 관리자 식별번호를 알고 있다면 비밀번호 변경 패킷을 임의로 변조하여 관리자 계정을 손쉽게 탈취할 수도 있다.

3) 스마트기기에 저장된 데이터의 비 암호화

스마트기기는 서버로부터 전송받은 정보를 저장하는 파일을 생성한다. 해당 파일에는 사용자 아이디와 성별, 키, 전화번호 등을 비롯한 각종 개인정보가 포함되어 있다. 그럼에도 불구하고, 해당 파일은 암호화가 되어 있지 않은 채 저장되어 있기 때문에 만약 모바일 기기 내 악성코드 감염이나 분실 시에는 개인건강정보를 포함한 개인정보가 손쉽게 유출될 수 있다.

4) 의료기기와 스마트기기 간 전송구간의 취약한 인증

측정기기와 스마트기기는 '블루투스 페어링'을 통해 측정된 개인건강정보를 주고받는다. 블루투스 페어링 시, PIN코드라는 일련의 숫자코드 사용하여 사용자를 인증한다. 그러나 해당 PIN코드가 항상 고정이 되거나 패킷에 그대로 남아 악의적인 공격자가 PIN코드를 이용하여 측정기기와 임의로 페어링을 맺을 수 있는 취약점이 발견되었다. 이 취약점을 이용하면 공격자는 고급기술이나 해킹에 대한 지식이 없어도 간단히 사용자의 개인건강정보를 탈취할 수 있다.

3. 피해규모 도출을 위한 위험분석

1) 위험분석을 위한 시나리오 구성

개인의 의료정보유출로 인한 피해규모를 산정하기 위해서는 시나리오를 먼저 작성한다. 사실에 기반을 두어 시나리오를 작성하기 위해서는 원격의료기기의 취약점 도출 단계에서 나온 취약점을 활용하여 시나리오를 작성하였다. 시나리오를 작성하기 위해 자산과 위협원의 식별을 먼저 수행하였다. 자산은 정보, 문서, 하드웨어, 소프트웨어, 인력, 서비스의 총 6개의 자산 분류 기준에 따라 식별할 수 있다. 정보 자산에는 개인건강정보와 개인정보, 기기정보 등이 있다. 소프트웨어 자산의 경우에는 앞서 의료기기 취약점 분석 시 사용하였던 관리 어플리케이션이 있고 서버, 네트워크 장비, 의료기기, 인증카드 리더기 등은 하드웨어 자산으로 분류하였다. 위협원은 내부정보유출자, 해커, 사이버 범죄기관(해커집단)으로 나눌 수 있다. 각각의 위협원은 목적이 다르므로 시나리오에 따라 위협원이 다르다. 이와 같이 식별된 자산, 위협원, 원격의료기기 취약점 그리고 최근 발생한 '약학정보원 개인정보유출 사례'를 기반으로 발생가능 한 시나리오를 작성하였다[27].

Table 3은 내부자에 의한 의료정보 유출사고에 대한 시나리오이다. 원격의료체계 기술적 안전성 평가기준 및 원격의료기기 취약점 문제점을 분석한 결과 대부분의 원격의료 현장에서 사용하는 시스템이 접근제어를 하지 않는 것으로 확인하였다. 따라서 권한이 없는 내부 임직원이 정보시스템에 접근하여 정보를 유출할 수도 있다. 피해규모는 원격의료 서비스를 이용하는 이용자가 200만 명으로 가정하였다. FAIR 방법론은 각각의 요소들이 1등급부터 5등급까지 구분하여 평가한다. 기댓값 이론을 적용하기 때문에 확률과 비용을 구하여 피해규모를 산출한다.

2) 확률구간의 도출

확률구간의 값은 위협원의 능력, 위협원의 위협빈도, 자산의 보안성을 고려하여 측정한다. Figure 9는 FAIR의 전체 프로세스를 나타낸 그림이다. 위협원은 정보자산에 접근권한이 없는 내부 임직원이므로 위협원의 능력은 조직에 평균적 직원 등급 수준, 즉 3등급으로 측정하였다. 위협원의 위협빈도는 정보시스템이 접근제어가 없는 시스템 이므로 2등급으로 측정하였다. 또한 자산의 보안정도는 기본적인 암호화 조치조차 이루어지지 않기 때문에 4등급으로 측정하였다. FAIR 프로세스에서 다음 단계의 값을 구하기 위해서는 Matrix 연산을 사용한다. Figure 10은 와 α의 β등급을 이용하여 A를 도출하는 Matrix의 예시이다. 제시하는 Matrix는 A를 도출하는 의 가중치를 같게 준

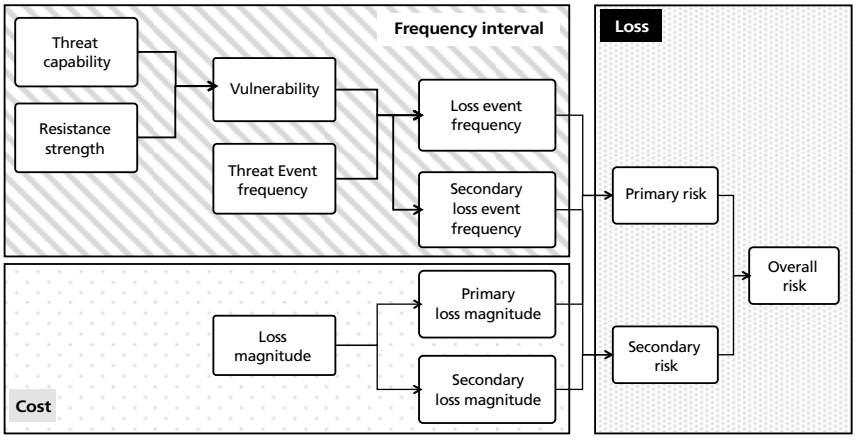

Figure 9. Factor analysis of information risk process based on scenario.

α	1	3	2	2	1	1
	2	4	3	2	2	1
	3	4	4	3	2	2
	4	5	4	4	3	2
	5	5	5	4	4	3
A		5	4	3	2	1
		β				

Figure 10. Matrix operation.

Table 4. Magnitude of loss

	Frequency interval	Cost	Min loss	Max loss
Operation cost	0.9-1.0	1,477	1,329.3	1,477
Response labor cost	0.9-1.0	931.6	838.4	931.6
Indemnity cost	0.9-1.0	40	36	40
Total	-	-	2,203.7	2,448.6

Unit: one hundred million won.

Matrix이다. 본 연구에서는 다음과 같이 모든 요소가 가중치를 같다고 가정하고 진행하였다. 이를 통하여 진행하면 vulnerability는 2등급, loss event frequency (LEF)는 1등급으로 도출하였다. LEF는 등급에 따라 확률구간을 가진다. 1등급의 확률구간은 0.9에서 1이다. 이는 사고가 발생할 확률이 매우 높다는 것을 의미한다. 또한, secondary loss event frequency는 LEF가 발생한 후에 발생할 수 있는 비용이므로 LEF와의 곱으로 구할 수 있다. 본 논문에서 제시하는 간접비용의 손해배상 청구비용은 최근 개인정보유출 사고 시 100%의 소송이 있었지만 LEF를 고려하여 0.9에서 1사이의 확률구간을 가진다[28].

3) 사고비용의 도출

사고비용은 직접비용과 간접비용으로 구분하여 도출하였다. 직접비용은 2013년 개인정보보호협회에서 발간된 자료에 의해 도출하였다[26]. 이 보고서에 따르면 의료시장의 정보유출 사고가 발생 시 정보 1건당 영업 손실은 73,850원 사고대응 인건비는 46,580원으로 제시하고 있다. 이용자를 200만 명으로 가정했기에 총 영업 손실은 14,770,000만 원이며, 대응인건 비용은 총 9,316,000만 원으로 도출된다.

간접비용은 최근 주요 개인정보 유출사고 소송결과를 보면 2011년 7월 SK컴즈에서 개인정보 유출로 인해 위자료 20만 원씩 배상한 사건이 있다[29]. 또한 KB금융사의 개인정보 유출사건으로 보았을 때, 소송 참여자 수는 총 피해자의 1% 수준으로 보인다. 따라서 200만 명 중 2만 명이 소송에 참여하고 SK컴즈 배상금인 20만 원으로 계산 시 4,000,000만 원으로 측정된다[30].

4) 피해규모의 도출

확률구간과 사고비용의 도출로 인하여 총 피해규모를 측정할 수 있다. 피해규모는 Table 4와 같이 확률구간을 고려하여 범위로 제시 할 수 있다. 시나리오를 이용하여 위험분석을 진행한 결과 위험이 매우 높은 등급으로 도출되었다. 특히 이 시나리오는 최근 발생한 '약학정보원 개인정보 유출' 사례와 유사하다는 점에서 의미가 있다. 분석 결과, 만약 유출사고가 발생한다면 약 2,200억 원에서 2,450억 원의 피해규모가 일어날 수 있음을 확인하였다.

고찰

2015년 5월 정부기관은 2014년 9월부터 2015년 3월까지 진행된 1단계 원격의료 시범사업에 대한 만족도에 대한

결과를 발표하였다. 전체 환자 중 84.3%가 원격모니터링이 만성질환관리를 위해 좋은 방법이라고 평가 하였다. 또한 기술적 안전성을 위해 접근통제 및 데이터베이스 암호화 등과 같은 보안 프로그램 등이 설치되어 해킹이나 개인정보유출 등 보안관련 사고는 발생하지 않았다고 발표하였다. 하지만, 적잖은 환자가 평가대상에서 누락되거나 해당 의료기관이 직접 설문을 조사하는 등의 신뢰성과 객관성이 지적 되었다. 기존 시범사업의 세부 과제로 4가지 이슈를 제시하였음에도 불구하고, 5월에 발표된 결과는 3가지에 대한 언급은 부재하고 나머지 1가지에 대해서만 결과를 내 놓았다. 특히, 사용자 인증을 통한 접근 통제, 데이터베이스 암호화 등과 같은 기술적 안전성에 대한 조치가 이루어지고 있다고는 했지만 정확한 결과를 발표하지 않아 신뢰할 수 없는 상태이다. 또한 아직 공개되지 않은 시범사업에 있어서 해킹이나 개인정보 유출사고가 없다고 판단하는 것은 매우 무리가 있는 판단이다.

이에 본 연구는 국민의 생명을 담보로 하는 원격의료에 대하여 기술적 안전성 수준을 진단할 수 있는 평가체계 수립을 목표로 하였다. 이에 원격의료체계 기술적 안전성 평가기준을 개발하고 개인의료정보 유출 시 환자나 기업 측면에서의 피해규모를 산정하였다. 기술적 안전성 수준을 진단하기 위해서 국내 · 외 관련 표준 및 법령을 분석하여 가장 높은 보안등급을 보장할 수 있는 평가기준을 만들었으며 피해규모를 산정하기 위해서는 최근 선진기업에서 가장 많이 사용하는 FAIR 방법론을 사용하여 위험분석을 진행하였다.

기존의 의료분야와 원격의료분야의 기준 및 세계적 기준을 수용하고, 법적기준을 제시할 수 있는 한국형 평가체계를 완벽히 수립하고자 한다면 정부 및 관련 의료기관의 지원이 뒷받침되어야 한다. 정보보호 및 기술적 안전성을 근원적으로 해결하기 위해서는 의료수가에 정보보호 비용과 개인건강정보보안 비용을 포함하는 정책이 반영되어야 할 것이다.

앞으로 원격의료 시장의 안전성을 확보하기 위해서는 안전성 인증제도가 도입되어야 할 것으로 보인다. 현재의 의료시장은 고객에게 더 나은 서비스를 제공하기 위해 다양한 종류의 서비스 및 의료기기를 사용하고 있다. 그러나 새로운 서비스 및 의료기기에 기술적 안전성에 대한 검증은 전혀 이루어지지 않은 채 무분별하게 사용되고 있다. 의료기기나 시스템의 사소한 취약점 하나가 전체에 영향을 끼칠 수 있다. 즉, 안전한 원격의료 시스템을 구축하기 위해서는 시스템 전반에 대한 '정보보호 관리체계' 인증 제도를 도입하는 것이 필요하다.

이와 같은 인증제도 운영을 위해서는 이해 관계자들 간의 협력 및 논의를 위한 생태계조성이 필요하다. 정부의 독자적 사업도입이 아닌 의료기관, 기술전문가, 의료인 등 다양한 측면에서 원격의료에 대한 논의가 이루어져야 한다. 또한, 원격의료를 시행함에 앞서 보안성 증대를 위한 충분한 예산, 시간, 정책지원이 이루어져야 할 것이다.

결론

원격의료는 IoT 환경과 정보화 시대에 발맞추어 매우 혁신적인 의료행위이다. 그러나 개인의료정보를 취급하면서 진단, 처방 등 환자의 생명에 영향을 줄 수 있어 기술적 안전성이 논란이 되고 있다. 환자의 개인의료정보를 보호할 수 있는 안전한 환경에서 원격의료가 진행되어야 한다. 모든 국민이 안전한 원격의료서비스를 이용하기 위해서 정부 및 관련 의료기관의 적극적인 관심과 지원, 정보보호에 대한 깊이 있는 이해 및 이를 뒷받침할 충분한 기술력이 확보되어야 한다. 기술적으로 안전한 환경에서의 원격의료서비스를 위해 본 연구에서 개발한 평가기준과 위험분석 방법이 정부 및 관련기관의 정책을 수립하는데 있어 도움이 되길 기대한다.

찾아보기말: 원격의료; 기술적 안전성 평가; 위험분석; FAIR 방법론

ORCID

Hee Joo Lee, http://orcid.org/0000-0003-2372-3327

Choi Nam, http://orcid.org/0000-0003-0076-7095
Jang Ho Yun, http://orcid.org/0000-0002-5759-567X
Jun Seob Yoon, http://orcid.org/0000-0002-7903-5753
Ho Jin Lee, http://orcid.org/0000-0002-3355-4144
Jin Suk Kim, http://orcid.org/0000-0002-0782-4518
Seok Yeong Kim, http://orcid.org/0000-0003-1611-5673
Jae Wook Choi, http://orcid.org/0000-0002-1996-7524
Kyung Ho Lee, http://orcid.org/0000-0002-5183-5927

REFERENCES

1. Ministry of Health and Welfare. Samsung Seoul Hospital existing outpatient prescription drug instructions [Internet]. Sejong: Ministry of Health and Welfare; 2015 [cited 2015 Aug 13]. Available from: http://www.mw.go.kr/front_new/al/sal0301vw.jsp?PAR_MENU_ID=04&MENU_ID=0403&page=18&CONT_SEQ=323565.
2. Lee SY. Telemedicine security vulnerability: goverment cover up? [Internet]. Seoul: Doctor's News; 2015 [cited 2015 Sep 28]. Available from: http://www.doctorsnews.co.kr/news/articleView.html?idxno=102025.
3. Choi ET. Doctor-patient liver telemedicine pilot project greatly expanded secondary propulsion [Internet]. Seoul: Dailypharm; 2015 [cited 2015 Aug 21]. Available from: http://www.dailypharm.com/News/194756.
4. Korean Medical Association. Korea Medical Association position on telemedicine pilot project for the evaluation of the Ministry of Health and Welfare [Internet]. Seoul: Korean Medical Association; 2015 [cited 2015 Aug 14]. Available from: http://www.kma.org/board2/view.php?w_seq=5838&page=7&kind_code=2.
5. Kim HJ. Physician licensing issue on telemedicine in the United State. KNU Law J 2014;47:543-570.
6. Ministry of Health and Welfare. It appears as high as telemedicine overall satisfaction 77% (91.8% more than average) [Internet]. Sejong: Ministry of Health and Welfare; 2015 [cited 2015 Aug 14]. Available from: https://www.library.uq.edu.au/training/citation/vancouv.pdf.
7. Lee JY. Korean u-Health Pilot Project implementation status and implications. Jincheon: Korea Information Society Development Institute; 2008.
8. International Organization for Standardization. Information security management. Geneva: International Organization for Standardization; 2013. (ISO/IEC 27001: 2013).
9. Freund J, Jones J. Measuring and managing information risk: a FAIR approach. Burlington: Elsevier Science; 2014.
10. Korea Internet and Security Agency. Korea-Information Security Management System. Seoul: Korea Internet and Security Agency Standard; 2013.
11. Personal Information Protection Act of 2015, Act No. 13423 (March 29, 2011).
12. Act on Promotion of Information and Communications Networks Utilization and Information Protection, ETC of 2014. Act No. 13014 (May 12, 1986).
13. Medical Service Act of 2015, Act No. 13108 (March 20, 1962).
14. International Organization for Standardization. Code of practice for information security controls. Geneva: International Organization for Standardization; 2013. (ISO/IEC 27002: 2013).
15. International Organization for Standardization. Information security management in health using ISO/IEC 27002. Geneva: International Organization for Standardization; 2008. (ISO 27799: 2008).
16. Health Insurance Portability and Accountability Act of 2013, Pub. L. No. 104–191 (August 21, 1996).
17. National Institute of Standard and Technology. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. Gaithersburg: National Institute of Standard and Technology; 2008. (NIST 800-66: 2008).
18. International Organization for Standardization. Health informatics: telehealth services: quality planning guidelines. Geneva: International Organization for Standardization; 2014. (ISO/TS 13131: 2014).
19. Austrian College of Rural & Remote Medicine. ACRRM Telehealth Advisory Committee standards framework [Internet]. Brisbane: Austrian College of Rural & Remote Medicine; 2012 [cited 2015 Oct 27]. Available from: http://www.ehealth.acrrm.org.au/system/files/private/ATHAC%20Telehealth%20Standards%20Framework_0.pdf.
20. American Telemedicine Association. Practice guidelines for video-based online mental health service [Internet]. Washington, DC: American Telemedicine Association; 2013 [cited 2015 Oct 27]. Available from: http://www.americantelemed.org/docs/default-source/standards/practice-guidelines-for-video-based-online-mental-health-services.pdf?sfvrsn=6.
21. American Telemedicine Association. Core operational guidelines for telehealth services involving provider-patient interactions [Internet]. Washington, DC: American Telemedicine Association; 2014 [cited 2015 Oct 27]. Available from: http://www.americantelemed.org/resources/telemedicine-practice-guidelines/telemedicine-practice-guidelines/core-operational-guidelines-for-telehealth-services-involving-provider-patient-interactions.
22. Australian Health Practitioner Regulation Agency. Good medical practice: a code of conduct of doctors in Australia [Internet]. Canberra; Australian Health Practitioner Regulation Agency; 2011 [cited 2015 Aug 21]. Available from: http://www.ahpra.gov.au/Search.aspx?q=good%20medical%20practice.
23. Ministry of the Interior. The standard for security measure of personal information. Seoul: Ministry of the Interior; 2014.
24. Korea Communication Commission. The standard for physical, technological, administrative measures. Seoul: Korea Communication Commission; 2015.
25. Ponemon Insuitute. 2011 Cost of Data Breach Study: United States [Internet]. Michigan: Ponemon Insuitute; 2012 [cited 2015

Oct 30]. Available from: http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf.

26. Jung SH, You JH, You BJ, Han CH, You SD. Analysis of social costs in the value of personal information and privacy [Internet]. Seoul: Personal Informations Protection Commission; 2013 [cited 2015 Aug 23]. Available from: http://www.prism.go.kr/homepage/researchCommon/retrieveResearchDetailPopup.do?research_id=1079930-201300001.
27. Kim KA. Hospital medical information is collected without knowing suffer significant damage [Internet]. Seoul: The Boannews; 2015 [cited 2015 Aug 22]. Available from: http://www.boannews.com/media/view.asp?idx=47158.
28. Heo SU. Several legal issues on private information leakage lawsuits: mainly about the methodology of finding law in hard cases. Justice 2009;110:302-331.
29. Kim TH. SK Communications, hacking 200,000 Korean won per victim compensation [Internet]. Seoul: The Boannews; 2013 [cited 2015 Aug 22]. Available from: http://www.boannews.com/media/view.asp?idx=34857&kind=3&search=title&find=20%B8%B8%BF%F8.
30. Kim GR. Personal information leakage incidents KB card only 1% of the victims would lawsuit [Internet]. Seoul: The Hankyoreh; 2014 [cited 2015 Aug 15]. Available from: http://www.hani.co.kr/arti/economy/finance/622409.html.

Peer Reviewers' Commentary

의학기술의 발전 역사 관점에서 볼 때 신의학기술, 보건 의료 기기 개발 그리고 신약개발 과정에서 필연적으로 환자안전과 경제적 이익과의 갈등의 발생은 피하기 어렵다. 즉 보건의료 전문가와 환자 그리고 보건의료산업계간의 갈등은 역사적으로도 중요한 이슈였으며 환자안전성과 과학성이 담보되지 않는 신의학기술이나 신약은 인정할 수 없는 것이었다. 최근 대두하고 있는 원격의료 역시 새로운 보건의료 기술의 도입 과정에서 일부 격오지 환자들의 의료서비스 접근성 향상과 동시에 원격의료의 기술적 안전성, 임상적 유효성과 환자안전성을 반드시 사전 검증하여야만 한다. 본 논문은 현 원격의료 시범사업의 기술적 안전성과 그로인한 정보유출의 위험성이 매우 크고 현재 우리나라 기술적 상황을 고려할 때 경제적 손실 규모가 천문학적으로 소요될 것임을 보여주고 있다. 향후 원격의료 도입 추진 과정에서 제도의 긍정적인 측면과 더불어 환자안전성과 임상적 유효성이라는 본래 목적을 달성할 수 있도록 하기 위해서는 의료제공자와 환자들의 주도하에 원격의료 사업의 설계와 검증을 철저히 하여야 함을 본 연구가 보여주고 있어 매우 시사하는 바가 크다.

[정리: 편집위원회]