디지털산업정보학회 논문지 제12권 제3호-2016년 9월
http://dx.doi.org/10.17662/ksdim.2016.12.3.087

개인정보보호관리체계(PIMS)를 이용한 의료정보보호 개선 방안 연구

: 의료기관 종사자를 중심으로*

민 경 은** · 김 성 준***

A Improvement Study on the Medical Information Protection Using Personal Information Management System(PIMS) : Focus on medical practitioners

Min Kyeongeun · Kim Sungjun

〈Abstract〉

This study intends to present an effective and efficient development plan about the information protection of medical institutions, by establishing the improvement plan about Personal Information Management System(PIMS) appropriate to the characteristics of medical information focusing on medical institutions generating and using domestic medical information, and doing an empirical study on medical information protection plan. For this, in view of the medical characteristics of the existing Information Security Management System(ISMS), the study presented a study model appropriated to medical institutions based on Personal Information Management Systems index specialized for personal information, and through this, presented the vulnerability diagnosis and vulnerability improvement plan. Based on ISMS index, it designed an improvement index of personal information protection management about each index. The study conducted a survey for executives and employees about PIMS. Accordingly, it presented vulnerability diagnosis items of the current management system indexes from the viewpoint of the people who establish and mange the personal information protection about patients' medical information targeting executives and employees who serve at hospitals and can access medical information.

Key Words : PIMS, ISMS, Medical Information

Ⅰ. 서론

최근 개인의 의료기록은 환자의 원무기록, 영상정보, 병원업무 전산화 등 의료정보화가 발전됨에 따라 의료정보의 발전 속도가 빨라지고 있다[1]. 이에 따라 병원의 정보환경에 역시 의료정보를 기반으로 하는 다양한 서비스 모델이 등장하며 개인의 의료정보 분야는 혁신적인 변화를 일으키고 있다. 또한 정부에서는 소비자 중심의 보건의료서비스 질을 향상하기 위

* 이 논문은 2016년도 산업통산자원부 산업보안 특성화학과 육성 사업 지원을 받아 수행된 연구임.
** 남서울대학교 산업보안학과 석사과정(주저자)
*** 남서울대학교 산업보안학과 교수(교신저자)

해 관련 정보 시스템 구축과 국가 차원에서의 보건의료정보화사업을 추진하고 있다[2-4].

의료정보는 언제 어디서나 어떤 질병에 대하여 어떻게 치료를 받았는지에 대한 정보를 포함하고 있는 개인의 사적인 내용으로 개인의 의료정보는 “의료법”, “형법”, “민법” 등의 법률에 따라 보호를 받고 있다[5].

의료정보는 보험 상품 및 진료 위치 추적 등의 용도로 활용될 수 있고 처방 약품 시장 현황, 매출 추이 분 석, 주요 질병 발생 추이 등 다양한 형태로 가공되어 제 약사 영업 전략과 신약 개발 방향 등을 수립하는데 활 용 될 수 있다[6].

송화진[7]의 연구에서는 지방의료원의 정보화 예산 편성 비율을 분석하였을 때 평균적으로 2,44%로 확인되었는데 이는 금융권의 정보화예산 대비 정보보호 예산 의무화 7%에 비교하여 볼 때 정부가 권장하는 비율 5%에 비해 매우 부족한 수치를 보여주었다. 또한 Identity Theft Resource Center[8]의 발표에서는 금융, 일반기업, 정부, 의료분야에 유출사고 중 43.1%가 대부분 의료분야가 공격대상이 되고 있음을 알려주었다. OECD[9]에 따르면 뉴잉글랜드에서 보건의료 전산자료 교환 네트워크를 통해 1998년 7월부터 2000년 2월까지 거래된 100만건 당 회원 연간 비용이 1,040만 달러(약 128억)에서 140만 달러(약17억)로 90%나 감소했다.

의료산업에 있어서 의료정보는 단순히 환자의 병원진료 기록, 영상기록의 차원을 넘어서 공공 및 민간 분야에서 다양하게 활용될 수 있다. 임상의 경우 의료정보를 활용하게 된다면 데이터 활용 및 분석, 보건의료 R&D, 공공보건 부문에 비용 절감이 가능하다. 또한 의료정보가 활용 될 수 있는 보험, 제약회사 웨어러블 기기 산업분야에서도 스마트의료와 헬스케어 산업 관심이 증가됨에 따라 민감한 의료정보는 다양한 곳에서 쓰일 수 있다. 앞으로 의료산업의 관심은 개인의 민감 정보인 의료정보를 활용하는 방향으로 흘러갈 것이다. 의료 산업의 시장은 점점 더 커지고 단순히 병원이 아닌 다국적 기업에서도 의료정보를 활용하는 측면은 강조되고 있지만 개인이 가장 우려는 하는 부분 역시 보안상의 문제이다. 의료정보의 유출이 된다면 개인에게 악영향을 줄 것 이다. 하지만 현재 국내에서는 의료정보를 다루는 병원경영진과 의료정보 관리 종사자의 정보보호인식 부재 및 개인정보보호에 대한 관리 수준을 향상시키기 위한 연구가 매우 빈약한 실정이다. 특히 의료정보에 대한 의료기관에 적합한 기존 정보보호 관리체계에 관한 실증연구가 거의 없는 실정이다.

최근까지의 의료정보 관련 연구들은 의료정보를 법적인 측면에서 다룬 연구가 주를 이루고 있다[1, 5, 10]. 또한 의료정보 보호를 위한 기술적인 방법에 초점을 맞추어져 연구가 진행되어 왔다[4, 11-14]. 의료분야에 대한 개인정보 관련 정책 및 의료정보화 시장 현황에 대한 연구가 주를 이루고 있는 실정이다[3, 7, 15-17].

본 연구의 차별점은 이상의 논의를 바탕으로 크게 4가지로 구분된다. 첫째, 의료기관 종사자 측면에서의 현행 의료정보 취약 요인들을 고찰하고, 국내 병원의 경쟁력 강화 및 개인정보보호 활성화에 대해 전략적인 제언하고자 한다. 둘째, 의료정보에 대해 개인정보 체계 구축을 위한 개선방안을 연구하기 위해서는 의료정보에 접근이 가능한 의료기간 종사자들에 대한 개인정보보호 인식 및 관리체계 준수여부 등의 여러 가지 특성을 복합적으로 살펴보기 위해 PIMS와 ISMS를 기반으로 부족한 부분을 파악하기 위한 연구가 필요하다. 셋째, 추후 적용되는 의료기관의 개인정보보호 관리체계에 대해 물리적, 관리적, 기술적인 부분에 대해 일괄적으로 적용되는 부분이외에도 의료정보의 특성을 고려해 정보보호체계 지침에서 추가적으로 수정 보안한 개선방안을 마련하는 것이 매우

중요하다. 넷째, 의료기관의 보안관리체계의 취약점 진단 및 개선방안을 제시하여 개인정보 관리체계 준수를 위한 방안과 논의가 되어져야 하겠다.

본 연구의 목적은 국내 의료정보를 담당하고 있는 국내 의료기관을 대상으로 하여 의료정보보호를 위한 적합한 개인정보관리체계를 구축 및 개선하여 이에 대해 의료정보를 활용함에 있어 개인정보의 유출 가능성을 최대한 차단하는 방안에 대한 연구하고자 한다. 이에 대해 의료기관 종사자들에게 설문조사를 함으로써 의료정보 관리시스템에 개인정보보호를 위한 효과적이고 효율적인 서비스 발전방안을 제시하고자 한다.

본 연구의 구성은 다음과 같다. 제Ⅱ장에서는 의료정보의 정의와 특성 그리고 시장 현황과 개인정보보호평가를 정리하고, 기존 의료정보의 선행연구를 살펴본다. 제Ⅲ장에서는 개인정보보호관리체계 개선방안에 대한 내용을 정리하고. 제Ⅳ장에서는 설문결과에 대해 표본 특성과 개선방안에 대해 기술하였다. 제Ⅴ장에서는 개인정보보호 관리체계의 개선방안에 대한 연구결과 및 시사점, 향후 연구방향에 대해 논의하였다.

Ⅱ. 이론적 배경

2.1 의료정보

의료정보란 의사와 의료종사자가 환자에게 진료행위를 하면서 진단, 치료행위, 치료경과에 따른 수집된 자료를 말한다[5]. 또는 개인의 과거, 현재, 미래의 육체적, 정신적 건강상태, 의료서비스를 받았던 사실 및 의료서비스에 대한 대가의 지급사실과 인구통계학적 사실 등을 담고 있는 자료라고 정의 할 수 있다[18].

개인의료정보는 개인의 병력사항과 같은 민감 정보로 타인에게 공개될 경우에 개인의 민감한 정보 유출과 더불어 대인관계 및 근로관계에서 불이익과 차별을 받을 수도 있는 등의 다양한 피해를 유발시킬 수 있다[7]. 의료정보에는 환자의 기초정보에서부터 환자의 건강정보, 진단 기록을 데이터베이스로 한 환자의 여러 정보 형태가 있으며, 이는 의료법상에서 보호되며, 의료기관과 보험회사는 정보 주체의 정당한 범위 내 에서만 사용이 가능하다[19]. 의료정보는 환자와 의사간 진료, 수술, 처치 등의 과정을 중심으로 작성되어 진료행위 외에도 접수, 수납, 보험의 업무내용이 포함되는 진료정보와 개념적 이해가 제한적이다[20].

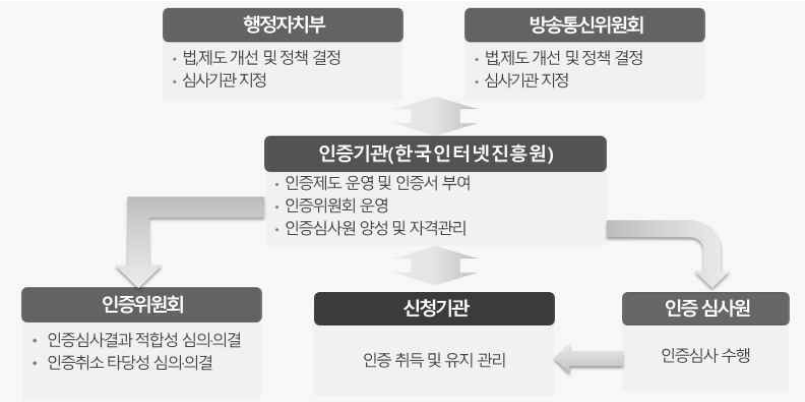
이명길[3]의 연구에서는 공공의료 기관을 대상으로 보건의료정보시스템 구축이 보건의료서비스를 효율적으로 적용하는 방안, 건강정보 활용에 대한 인식도, 선호도에 대한 의견을 수렴해 정책방향에 대한 연구를 진행하였다. 노문종[21]의 연구에서는 환자의 의료정보의 공유를 위한 작업의 일환으로 대학병원의 진료정보 공유시스템을 정보공유를 중심으로 분석하고 IHE(Integrating the Healthcare Enterprise)에서 새롭게 제시한 XDS(Cross-Enterprise Document Sharing)를 분석하여 prototyping을 구축하고 그 결과를 통해 기존 진료정보 공유시스템과 비교・분석하였다. 윤성태[12]의 연구에서는 병원에서 관리하는 개인의료정보에 대해 국내외 의료 관련 규제, 모바일 허가 가이드라인의 보안 규정 항목과 의료 선진 규정의 보안 항목을 분석하고 ISO/TC215 WG4 국제 표준기구에서 제시하고 있는 선진 의료정보 보안 표준 규격들의 국내외 규정을 비교 분석하여 통합적으로 참고할 수 있는 보안 기준 항목을 정리 및 보안 기술 적용 방법과 국제 표준 규격 이해를 통한 보안 운용 방안을 아래와 같이 3종류로 나누어 고찰하였다.

2.2 개인정보보호관리체계(PIMS)의 이론적 고찰

개인정보보호관리체계(PIMS: Personal Information/privacy Management System)는 개인정보에 특화해 기업이 고객들의 개인정보를 보호 활동을 지속적이고 체계적으로 수행하기 위한 체계를 지칭한다[22]. 개인정보보호관리체계는 개인정보보호를 위해 일정 수준 이상의 관리적 기술적 물리적 대책을 수립 및 운영하고 있을 경우 인증을 부여하는 체계이다[23].

국내에서는 PIMS 인증제도가 2011년부터 한국인터넷진흥원(KISA)을 인증기관으로 하여 기업의 개인정보 보호활동을 체계적이고 지속적으로 수행하기 위해 필요한 보호조치체계를 구축하였는지 점검하고 일정 수준 이상의 기업에 인증을 부여하고 있다[24]. PIMS의 인증심사는 받는 종류에 따라 최초심사, 사후관리, 갱신 심사로 구분한다[25]. PIPL와 제도가 통합됨에 따라 인증항목은 동일하지만 기관의 규모에 따라 소규모 기업, 중간규모 기업, 대기업, 공공기관으로 구분하여 인증 받는 항목 수에 차등을 두고 있다[26]. 개인정보보호관리체계는 이용자 및 정보주체는 해당 기관의 인증취득 여부를 통해 개인정보의 누출가능성을 최소화하고 효과적으로 보호하고 있음을 갈음하는 수단이 되고 있다[23]. PIMS의 관리구성은 아래 <그림 1>과 같이 수행된다.

심미나[27]의 연구에서는 국내 PIMS 도입에 예상되는 기존 ISMS와 중복성에 관한 연구하며 이에 대한 해소방안을 제시하며 PIMS나 ISMS 도입을 계획하는 조직은 보다 효율적으로 정보보호와 개인정보관리 활동을 수행할 수 있고, 비용-효과적이고 차별화된 인증제도 도입이 가능하다는 연구내용을 제안하였다. 채은지[28]의 연구에서는 고객의 개인정보를 보유하고 있는 금융회사가 기업 내부자에 의한 개인정보 유출을 방지하기 위한 시스템을 구축하는데 필요한 방법론을 제시하였다. 또한 구축사례를 통해 구현 가능성을 확인하였으며 향후 타 산업분야 또는 동일한 요구사항이 있는 회사에서도 활용할 수 있도록 필요한 내용과 절차를 체계화 하였다. 차건상 외[29]의 연구에서는 공공기관 및 민간기업의 개인정보보호담당자와 개인정보관리체계 인증제 관련 전문가를 대상으로 개인정보보호법상의 자율규제 확보를 위한 인증제 마련 시 고려사항을 도출하여 개인정보보호법상의 적용대상을 고려한 개인정보관리체계 인증제 도입 방안을 제시하였다.



<그림 1> PIMS 관리구성[25]

Ⅲ. PIMS기반의 의료정보 지침 개선안

3.1 의료정보 보호지침 개선의 필요성과 영역의 정의

3.1.1 의료정보 보안지침 개선현황

의료정보의 경우 개인들의 병원에서 진료를 받는 모든 정보를 포괄하는 개념으로서, 환자 개인이 생성할 수 있는 일반 의료정보는 공공 의료기관인 보건소와 병원과 더불어 보험회사 및 일반 제약회사에서도 다루어 질 수 있는 정보의 보유주체가 의료기관 종사자에 한정되지 않고 다양하게 활용 되는 정보에 해당한다. 이러한 의료정보가 유출 및 사이버 공격과 같은 사고가 발생한다면 이에 대한 피해를 받는 개인에게 끼치는 영향력은 사회적으로 상당한 문제를 야기 시킬 것이다. 그리고 의료정보의 중요도 측면에서 보다 그 중요성을 인식한 정보보호 운영・관리・감독을 보다 체계적으로 관리할 수 있는 표준 지침이 요구되며 각 기관에서는 이에 대한 지침마련 준수를 하여야 한다.

현행 의료법과 기타 법률 등에 따르면 의료정보에 대한 정보에 대한 관리・감독에 대한 규정을 다루고는 있지만, 의료정보의 특수성을 감안한 정보보호 체계에 대한 내용은 규정하고 있지 않다. 하지만 이번에 새롭게 개정된 미래창조과학부가 발표한 내용에 따르면 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(2016년 6월 2일 시행)'의 시행령 및 시행 규칙 개정안에 따라 해당되는 의료기관에 대해서는 입법예고 하였다. 이는 현재 의료분야에 대해서 법적인 의무로 적용받는 정보보호관리체계에 대해 국가적인 차원에서 처음으로 법적인 강제성을 띄고 있는 것에서 의미가 있다. 한국인터넷진흥원(KISA)에서 주관하는 정보보호관리체계(Information Security Management System)에 대해 개정안에 대한 발표 내용을 좀 더 살펴보면 정보보호 관리체계 인증 신규 의무 대상으로 매출 또는 세입이 1500억원 이상 업체 중 다량의 민감한 정보를 다루는 의료기관과 금융업이 포함되었다는 것이 주요 변경내용이다. 본 법률의 시행령에 따르면 해당되는 의료기관의 경우 ISMS와 유사한 인증인 정보보호 경영 시스템 인증(ISO/IEC 27001), 개인정보보호 관리체계(PIMS) 인증 및 주요 정보통신 기반시설 취약점의 점검 분석・평가 등을 받은 경우 심사 항목 일부를 생략할 수 있도록 하였다.

3.1.2 의료정보 보안지침 개선 필요성

의료정보 보호 지침개선안에 기존의 ISMS가 아닌 PIMS의 방법론을 적용한데는 다음과 같은 이유를 들 수 있다. 먼저 의료기관의 정보보호 관리체계 인증에 대해서는 의료정보가 가장 '민감'한 특성을 갖는 개인정보의 특성을 갖고 있기 때문에 개인정보 보호의 측면에서 개인정보 보호의 성질이 더 강하다고 볼 수 있기 때문이다. 의료정보 생성의 경우 의사 한명이 환자에 대한 모든 진료를 행하는 것이 아니라 다수의 의사, 간호사, 의료기사를 비롯한 의료기관 종사자들이 집단적으로 관여되는 의료행위에는 환자에 대한 의료정보의 공유가 필수적인 역할을 하고 있기 때문에 환자의 의료정보는 보다 다수가 공유를 하는 개인정보의 측면이 강하다고 볼 수 있다[30]. 둘째, ISMS보다는 의료정보의 특수성인 개인의 민감 정보라는 특수성을 고려하기 위해서 개인정보보호에 대해 자세히 규정하고 있는 PIMS의 세부항목을 생명주기의 내용이 포함된 의료정보 개인정보보호 관리체계의 개선안이 필요하다. 개인정보의 수집, 제공, 이용, 파기에 대한 내용이 보다 자세하게 적용 될 수 있다는 장점이 있다. 마지막으로 PIMS 인증대상 유형 중 인증 대상에 있어 기존의 PIMS에서 PIPL(Personal Information Protection Level)과 통합됨에 따라 주요

인증대상과 항목에 있어서 모든 인증대상에 해당하는 소규모 기업에 적용이 가능한 단일 인증항목을 평가가 필요하기 때문이다. 본 연구에서 정의하는 PIMS의 항목을 사용한다면 개정된 공공기관, 대기업, 중소기업, 소상공인 등 기존에 인증 신청기관의 규모에 따라 차등을 두고 있는 부분에 대하여 공통의 기준을 마련할 수 있다. 이에 본 개선안에서는 중소규모 기업을 중심으로 모든 항목에 적용받는 소상공인을 필수영역으로 구분하며, 모든 기관의 유형에 적용될 수 있는 인증을 받도록 개발하였다. 또한 PIMS에서 규정하고 있는 부분 외에 공통의 항목에 대해서는 정보보호 관리체계인 ISMS의 내용과 선행연구를 비교하여 추가영역에 내용을 보안하였다.

본 보안지침을 통해 기존에 정보보호 인증 선택에 있어 보안이 필요한 지표를 파악할 수 있고, 의료기관의 정보통신사업자 및 사업자들 모두에게 적용 할 수 있는 세부 지침항목을 제공할 수 있을 것으로 예상되며 이는 PIMS가 보다 현실성 있는 표준지침이 될 수 있다.

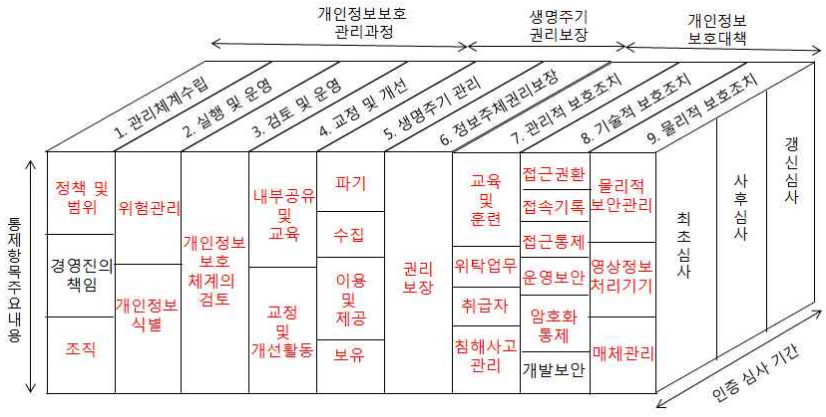
본 연구의 2장 선행연구를 통해 의료기관의 구성요소를 ISMS의 통제항목과 PIMS의 기본 통제항목인 개인정보보호 관리과정, 개인정보 생명주기, 개인정보 보호대책을 기준으로 의료정보보호에 있어 PIMS의 세부 항목 중에 개선내용을 기본으로 한 영역으로 구분하였다.

<그림 2>는 의료정보에 대한 세부적으로 보자면 3개의 관리영역 중 9개의 통제영역중 개인정보처리에 관한 프레임워크이다. 전문적인 IT 기술영역 부분과 공공기관, 대기업 등 대규모 기관에 해당하는 항목을 배제하였다. 해당되는 프레임워크의 항목은 기업의 규모에 따라 의료기관에 적용되는 항목을 선택하였다. <표 1>과 같이 기존의 모든 유형이 적용되는 유형 1의 47개의 필수 인증항목을 중심으로 유형 2의 중소기업에 해당하는 통제영역 20개 중 기존 74개 항목에 20개 항목의 내용을 ISMS의 통제항목, 선행연구, 관련 법률의 내용을 추가하여 분야별 점검항목에 수정 보안하였다.

3.2 PIMS기반의 의료정보 보호 지침 개선 항목

3.2.1 관리체계 수립의 항목

<표 2>는 관리체계 구성수립 항목이다. 의료기관 종사자에 대해 정보보호 관리체계의 구성은 의료정



<그림 2> 의료정보보호에 대한 PIMS 통제항목 프레임워크

<표 1> 보안 지침의 개선에 사용된 PIMS 점검항목[26]

분야	통제영역	세부점검항목	필수	추가	통제영역 / 세부점검 항목
개인정보 보호관리 과정	1. 관리체계 수립	3	6	2	1
	2. 실행 및 운영	2	5	1	2
	3. 검토 및 모니터링	1	2		1
	4. 교정 및 개선	2	2	1	1
생명주기 및 권리보장	5. 개인정보 생명주기 관리	4	15	15	7
	6. 정보주체 권리보장	1	4	4	2
개인정보 보호대책	7. 관리적 보호조치	4	10	7	3
	8. 기술적 보호조치	5	23	14	2
	9. 물리적 보호조치	3	7	3	1
총계		25	74	47	20

<표 2> 관리체계 구성수립 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
관리체계 수립	1.1.1 정책의 수립	개인정보보호정책과 시행문서를 수립하여 조직의 개인정보보호 방침과 방향을 명확하게 제시하여야 한다. 또한, 개인정보보호(관리)책임자 등 경영진의 승인을 받고 임직원 및 관련자에게 공표하여야 한다.	필수
	1.1.2 정책의 유지관리	개인정보보호정책 및 시행문서는 관련 법·규제를 준수하고, 상위 정책과 일관성을 유지하여야 한다. 또한, 정기적으로 검토하여 필요한 경우 제·개정 및 이력관리하고 운영기록을 생성·유지하여야 한다.	
	1.1.3 범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함하는 개인정보보호 관리체계 범위를 설정하여야 한다.	
	1.3.1 개인정보보호 관리책임자의 지정	지속적인 개인정보보호 관리체계 운영활동을 위하여 개인정보보호관리책임자를 지정하여야 한다.	필수
	1.3.2 조직의 구성	조직 협의체의 구성은 최고경영자가 관리체계를 업무 중요도에 대한 중요도 분석을 통해 지속적인 운영이 가능하도록 구성한다.	
	1.3.3 역할 및 책임	개인정보관리(보호)책임자 및 개인정보를 취급하는 각 부서의 책임자, 담당자에 대한 역할과 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다. 또한, 상호 의사소통할 수 있는 보고체계를 정의하여야 한다.	

보 보호와 정보 운영에 있어서 반드시 필요하다. 정보보호관리 책임자의 지정은 개인정보보호 정책 수립과 책임자의 역할에 따라 정보보호의 업무영역에 대한 내용은 모든 인증대상에게 적용되는 가장 중요한 항목이다. 필수적으로 관리체계 수립에 대해 정책 수립과 개인하지만 기존 PIMS에서 소상공인을 제외한 나머지 유형 중 조직의 구성 및 역할 책임에 대한 항목의 세부 점검 항목에 있어 정보보호 최고 책임자 지정, 실무조직 구성, 정보보호위원회 설치 등 선행논문의 내용과 ISMS의 업무 운영의 항목에 대해 인증 내용에 대해 추가하여 보안이 필요할 것으로 보인다. 이것은 정보보호 활동의 경영진의 역할과 관련 내용에 대한 업무영역을 명확히 하고, 보고체계 정비를 위해 필요하기 때문이다.

3.2.2 실행 및 운영에 대한 항목

<표 3>은 실행 및 운영의 항목에 대한 표이다. 개인정보에 대한 조직의 정보자산 식별과 정보운영에 있어 필수적으로 이행되어야 하는 항목이다. 이에 대한 조직의 개인정보보호대책 수립과 이행은 명확한 정의와 의료정보에 대한 위험관리는 경영진에 의해서 계획 수립과 정보보호 대책이 구현되어야 한다.

모든 인증 대상에 있어서 개인정보인 의료정보의

<표 3> 실행 및 운영에 대한 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
실행 및 운영	2.1.1 개인정보 식별	조직의 개인정보 및 개인정보 관련 자산을 식별하고 중요도를 결정하여 보안등급을 부여한 후 그에 따른 취급절차를 정의·이행하여야 한다. 또한, 자산별 책임 소재를 명확히 정의하여야 한다.	필수
	2.1.2 개인정보 흐름 파악	조직의 개인정보 관련 서비스 및 업무에서 개인정보 흐름을 파악하여 개인정보 흐름도(표)를 작성하고 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	
	2.2.1 위험관리 방법 및 계획 수립	조직의 개인정보보호 전 영역에 대하여 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리계획을 수립하여야 한다.	
	2.2.2 위험 식별 및 평가	위험관리 방법 및 계획에 따라 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.	
		- 보안등급과 취급 - 위험평가계획서 작성	
	2.2.2 이행계획 수립 및 보호대책 구현	위험을 수용 가능한 수준으로 감소시키기 위해 개인정보보호대책을 선정하고 이행계획을 수립하여 경영진의 승인을 받아야 한다. 또한, 수립된 이행계획에 따라 보호대책을 구현하여야 한다.	
		경영진은 이행결과의 정확성 및 효과성 여부를 확인하여 이에 대한 보호대책을 구현, 평가보고서 형식으로 확인해야 함	

<표 4> 검토 및 모니터링의 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
검토 및 모니터링	3.11 법적요구사항 준수검토	조직이 준수해야 할 개인정보보호 관련 법적 요구 사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.	
	3.1.2 내부 감사	개인정보보호 관리체계가 효과적으로 운영되고 있는지를 점검하기 위해 연 1회 이상 내부감사 계획을 수립하고 수행하여야 한다. 내부감사를 통해 발견된 문제점을 보완하여 경영진에게 보고하여야 한다.	
		이행여부 확인을 위해 독립성 및 전문성을 확보할 수 있는 보안감사조직을 구성, 감사, 대상, 범위, 방법을 고려한 감사계획을 수립. 내부감사계획 및 결과보고서 작성	추가

<표 5> 교정 및 개선 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
교정 및 개선점검	4.11 개인정보보호 개선 활동	주기적 또는 상시적으로 수행해야 하는 개인정보보호 활동을 문서화하여 그 운영현황을 지속적으로 점검·개선하는 등의 관리를 하여야 한다.	
	4.2.1 내부 공유 및 교육	개인정보 관리계획을 운영 또는 이행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.	필수
		개인정보를 처리하는 모든 부서 및 직원의 개인정보 보호에 대한 관련 교육을 시행한다. - 정보보호 교육 프로그램 수립, 대상, 내용 및 방법	추가

식별과 중요도에 따른 절차가 중요하다. 또한 보안등급에 따라서 책임 소재 정의의 내용은 명확히 해야 한다. 위험관리영역의 내용은 기업의 규모에 상관없이 정보보호를 위해 정보보호 관리대책이 필요한 영역으로 보고 정보자산에 대해 위험평가 계획서, 평가보고서, 평가이행 계획서 등으로 운영항목에 대한 절차를 문서로 작성해 업무의 이행여부를 평가 및 기록하여 저장 할 수 있도록 하여야 한다.

3.2.3 검토 및 모니터링 분류 항목

<표 4>는 검토 및 모니터링 분류 항목에 대한 표이다. 개인정보보호 관리체계에 있어서 조직은 법적인 요구사항을 이행하도록 하며, 정보보호에 대한 검토와 모니터링에 대해 내부감사를 통해 개인정보보호 관리체계의 운영을 점검을 할 필요가 있다.

특히 내부 감사의 경우 의료정보보호 조직에서는

<표 6> 개인정보 생명주기 관리 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
개인정보 생명주기	5.1.1 개인정보 수집 제한	서비스 제공을 위해 필요한 최소한의 정보만을 수집해야 한다. 개인정보 수집 시 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	필수
		법률에 특별한 규정이 있는 경우 또는 법령상 의무 준수를 위하여 불가피한 경우는 제외한다.	추가
	5.1.2 정보주체의 동의	개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체(이용자)의 동의를 얻은 후에 수집해야 한다.	필수
		동의를 받을 때 고지해야 하는 사항 - 개인정보의 수집·이용목적 - 수집하려는 개인정보의 항목 - 개인정보의 보유 및 이용 기간 - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	추가
	5.1.3 법정대리인 동의 및 고지	만14세 미만 아동의 개인정보를 수집할 경우 법정대리인에게 필요한 사항을 고지하고, 동의를 획득하여야 한다.	필수
	5.1.4 민감정보 및 고유 식별정보의 수집 제한	고유식별정보와 민감정보는 정보주체(이용자)의 별도 동의를 받거나 다른 법령에서 처리를 요구하여 허용된 경우를 제외하고는 수집할 수 없다.	필수
	5.1.5 주민등록번호 수집·이용 제한	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우를 제외하고 주민등록번호를 수집·이용할 수 없다.	필수
	5.1.6 주민등록번호 대체수단	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우에도 주민등록번호 대체수단을 제공해야 한다.	필수
	5.1.7 간접수집 보호조치	시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집 개인정보에 대하여 적절한 보호대책을 수립·이행해야 한다.	필수
	5.1.8 개인정보처리(취급) 방침	개인정보처리(취급)방침을 수립하여 정보주체(이용자)가 언제든지 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	필수
	5.2.1 개인정보 제3자 제공	개인정보를 제3자에게 제공 시, 관련내용을 고지하고 동의를 획득한 후 제공하여야 하며, 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제해야 한다.	필수
		의료법 21조에 해당되는 경우이외는 제공할 수 없으며, 다음과 같은 항목을 정보주체의 별도의 동의를 받아야 하며 다음 항목을 고지 - 개인정보를 제공받는 자 - 개인정보의 이용 목적(제공시에는 제공받는 자의 이용 목적) - 이용 또는 제공하는 개인정보의 항목 - 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용기간) - 동의를 거부할 권리가 있다는 사실과 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	추가
		다른 법률에 특별한 규정이 있는 경우에 대해 예외로 해야 한다. - 정보주체로부터 별도의 동의를 받은 경우 - 다른 법률에 특별한 규정이 있는 경우 - 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 - 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 - 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 - 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 - 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 - 법원의 재판업무 수행을 위하여 필요한 경우 - 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우	추가

	5.2.2 제공받은 개인정보의 관리	개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않고 제3자에게 제공하지 않아야 하며, 개인정보를 안전하게 관리하여야 한다.	필수
	5.2.3 개인정보 목적 외 이용 및 제공	개인정보를 정보주체(이용자)에게 고지·동의 받은 범위에서 벗어나지 않도록 이용하여야 하며, 만약 동의 범위를 벗어날 경우 정보주체(이용자)로부터 추가 동의를 획득하고, 적절한 보호조치를 하여야 한다.	필수
	5.2.4 개인정보의 이전	영업의 양도, 합병 등으로 개인정보를 이전하는 경우 적절한 보호대책을 수립·이행해야 한다. 또한, 개인정보를 해외로 이전하는 경우 개인정보에 대한 적절한 보호대책을 수립·이행해야 한다.	필수
		의료법 21조 3항에 해당되는 경우로 제한하며 정보주체에게 이전하는 의료기관은 다음 사항을 통지 - 개인정보를 이전하려는 사실 - 개인정보를 이전받는 자(영업양수자 등)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처 - 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차	추가
	5.3.1 개인정보 품질 보장	수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성, 완전성, 최신성을 유지 하여야 한다.	필수
	5.4.1 개인정보 파기 규정 및 절차	개인정보의 보유기간 및 파기와 관련한 내부 규정을 수립하고, 파기 관련 보호조치를 마련하여야 한다. 또한, 개인정보 수집 동의 등에 대한 기록은 탈퇴 전까지 안전하게 보관하여야 한다.	필수
		민간 의료기관 개설자가 폐업 또는 휴업 신고를 할 때에는 기록·보존하고 있는 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 관할 보건소장에게 넘겨야 함	추가
	5.4.2 개인정보의 파기	개인정보의 수집 목적이 달성된 경우, 안전한 방법으로 지체없이 파기하고 관련 사항은 기록 관리하여야 한다. 개인정보의 수집목적 달성 후에도 관련 법령 등에 의해 보유가 필요하다면 정보주체(이용자)에게 고지하고 최소한의 항목을 보유해야 한다.	필수
		의료법 시행규칙 15조에 따라 의료기관의 개설자 또는 관리자는 의무기록심의와 같은 내부심의를 거쳐 의료기록을 보존할 수 있으며, 기간이 수집목적을 달성한 진료기록 등 의료정보에 대해서 지체 없이 파기가 바람직하다. 이에 대해 진료정보를 연장하여 보관하는 경우 정보주체가 의료기관에 개인정보의 삭제를 요청하며 개인정보보호법 36조에 따라 필요한 조치를 취한 후 주체에게 고지하여야 한다.	추가

이행여부 확인을 위해 독립성 및 전문성을 갖춘 외부 조직이나, 공공기관의 감사를 통해 정보보안감사 조직을 운영을 구성하여, 정보 감사, 대상 범위, 방법을 계획의 내용을 인정받아야 할 필요가 있다. 이 역시 내부감사계획 및 결과보고서를 통해 개인정보보호 활동에 대한 내용을 문서화 하여, 운영 점검 개선의 필요성이 요구 된다.

3.2.4 교정 및 개선 항목

<표 5>는 교정 및 개선 항목에 대한 표이다. 개인정보보호 활동의 영역에서 가장 중요한 요인으로 볼 수 있는 영역으로 개인정보보호 개선활동, 내부공유 및 교육의 내용을 정의하는 항목이다. 본 항목을 통해 개인정보보호 활동의 내용은 개선활동의 일환으로 운영 현황을 점검 개선하여야 한다. 특히 정보보호 담당자와 관련 부서에 대한 정보보호 교육에 대한 항목은 필수적으로 이행하여야 한다. 추가적으로 정보보호 교육 프로그램 수행 및 대상과 관련 내용, 방법에 대한 정의가 요구된다.

3.2.5 개인정보 생명주기 관리 항목

<표 6>은 개인정보 생명주기 항목에 대한 표이다. PIMS의 가장 큰 특징으로 모든 인증대상은 반드시 개인정보 수집 시 보호조치, 이용 및 제공, 보유 시 보호조치, 파기 시 보호조치 등에 대해 필수적으로 이행되어야 한다.

특히 정보 제공에 대한 항목은 의료정보의 경우 정보 공유가 되는 부분에 있어 제 3자제공과 제공받는 개인정보의 관리영역에 해당하는 경우 접근 통제, 암호 통제, 운영보안 내용 이행 등의 기술적인 부분이

<표 7> 정보주체 권리보장치 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
정보주체 권리보장	6.1.1 개인정보 열람	개인정보에 대한 열람・정정・삭제 방법 및 절차를 제공하고, 정보주체(이용자)가 요구 시 열람하게 하여야 한다.	필수
		단 환자의 기록에 대해서는 「의료법」 제21조(열람요구 등)에 따라 열람요구를 처리해야 한다.	추가
	6.1.2 개인정보정정・삭제	정보주체(이용자)가 개인정보에 대한 정정・삭제 요구 시 지체없이 처리하고, 기록을 남겨야 한다. 또한, 개인정보 이용내역을 법령에 따라 주기적으로 통지하여야 한다.	필수
	6.1.3 개인정보 처리 정지	정보주체(이용자)에게 개인정보에 대한 처리정지 방법 및 절차를 제공하고, 처리정지 요구 시 지체없이 처리하고, 기록을 남겨야 한다.	필수
		진료기록부, 조산기록부, 간호기록부에 기재되어 있는 개인정보는 의료법 시행규칙에 근거하여 수집되고 있으므로 환자는 그 삭제를 요청할 수 없음 의료법에서 정한 보관기간이 경과한 진료기록에 대해서는 정정・삭제 요구 시 이에 응하여야 한다.	추가
	6.1.4 권리행사의 방법 및 절차	정보주체(이용자)가 열람 등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 상담창구 등 필요한 절차를 마련하여야 한다.	필수

이행되어야 한다. 또한 의료정보의 특성상 개인정보의 파기와 이전에 해당하는 경우 해당되는 의료법 제15조 시행 규칙(진료에 관한 기록의 보존)과 제 33조에 따라 수집 목적의 달성된 경우라도 보관을 요구하는 기록 저장기간과 진료기록의 이전에 대해 다른 법률을 적용받는 부분에 대한 정보지침이 개정이 필요하다.

3.2.6 정보주체 권리보장 항목

<표 7>은 정보주체 권리보장 항목에 대한 표이다. 개인정보는 자기결정권의 따라 대한민국 헌법상의 권리로 국가권력으로부터 간섭 없이 일정한 사적사항에 관하여 스스로 결정할 수 있는 자의적 권리를 갖는다. 하지만 최근 의료정보의 경우 환자의 자기결정권과 관련 법률에 있어서 권리 보장에 대해 법적 충돌이 발생되는 경우가 생기고 있다. 이에 개인정보 열람, 정보정정・삭제 처리 정지 및 권리행사의 방법 및 절차 등에 대해 정보주체의 권리보장의 영역은 이에 대한 추후 논의가 필요하다.

3.2.7 관리적 보호조치 항목

<표 8>은 관리적 보호조치에 대한 표이다. 개인 개인정보 보호대책의 경우 관리적, 기술적, 물리적 보호조치 중에 관리적 보호조치는 대부분의 적용유형 항목에 있어 교육 및 훈련, 취급자 관리, 위탁업무, 침해사고 관리에 모든 유형이 필수적으로 해당되는 영역이라 교육 및 훈련의 내용에 대해 교육 대상에 대한 세부적인 내용을 정의하며, 이에 대한 모든 내용을 포함하고 직무별 전문성 제고에 대한 적합한 교육 방법에 대한 내용을 추가적으로 개선되어야 한다. 또한 위탁자 관리, 감독에 있어서도 위탁 업체에 대해 보안요구사항을 정의, 이행관리, 계약이행여부에 대한 검토가 필요하다.

3.2.8 기술적 보호조치 항목

<표 9>는 기술적 보호조치에 대한 표이다. 기술적 보호조치는 기술적인 영역의 특성상 기술적인 기반(인력, 예산)등이 있는 공공기관과 대기업 조직에 해당되는 유형이 많으므로 이에 대한 현실적으로 유형화시키기에는 어려운 부분이 많다. 이에 대해 공통적으로 적

<표 8> 관리적 보호조치 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
관리적 보호조치	7.1.1 교육 및 훈련 시행·평가	연간 개인정보보호 교육 계획을 수립하고, 관련 임직원 및 외부자를 대상으로 주기적인 교육을 시행하여야 한다. 또한, 교육 시행에 대한 기록을 남기고 결과를 평가하여 다음 교육에 반영하여야 한다.	필수
		교육대상에는 관련 조직내 직원 및 외부자(의료정보를 관리 운영하는 수탁자)를 모두 포함한다. 교육에 대한 내용은 관리체계 개요, 내부 규정 및 절차, 법적 책임 등의 모든 내용을 포함하고 직무별 전문성 제고에 적합한 교육내용 및 방법에 따라 시행한다.	추가
	7.2.1 개인정보 취급자 감독	개인정보를 취급하는 임직원 및 외부자를 최소한으로 제한하고 개인정보취급자 목록을 관리하여야 한다. 또한 개인정보보호 책임의 충실한 이행 여부에 대해 상벌 규정을 마련하여야 한다.	필수
	7.2.2 보안 서약서	개인정보를 취급하는 개인정보취급자, 임시직원, 외부자 등에게 보안서약서를 받아야 한다.	필수
	7.2.3 퇴직 및 직무변경 관리	개인정보취급자의 퇴직 및 직무변경 시 자산반납, 계정 및 권한 회수·조정, 결과 확인 등의 개인정보취급자 인사 관리 절차를 수립하고 이행하여야 한다.	추가
	7.3.1 외부 위탁 계약	개인정보 처리업무를 외부에 위탁하는 경우 개인정보보호에 관한 요구사항, 관리감독, 법규정 위반의 배상책임 등에 관한 사항을 계약서 등에 문서화하여야 한다.	필수
		개인정보 처리 위탁 계약서 기재사항 - 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 - 개인정보의 기술적·관리적 보호조치에 관한 사항 - 위탁업무의 목적 및 범위 - 재 위탁 제한에 관한 사항 - 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 - 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 - 법 제26조제2항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항	추가
	7.3.2 정보주체 고지	개인정보 처리업무 위탁시 수탁자, 수탁목적 등 관련사항을 정보주체(이용자)에게 고지하고 필요한 경우 동의를 받아야 한다.	필수
	7.3.3 위탁자 관리·감독	위탁 업체가 계약서 및 서비스 수준 협약, 관련 법·규정 등에 명시된 사항을 충분히 이행하는지 주기적으로 관리·감독해야 한다.	필수
		보안요구사항 정의, 보안이행관리, 계약 만료 시 보안 이행여부 검토	추가
	7.4.1 침해사고 대응절차 및 체계구축	개인정보 침해사고 대응절차를 수립하고, 개인정보 침해사고 대응이 신속하게 이루어질 수 있도록 대응체계를 구축하며 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.	
	7.4.2 침해사고 훈련 및 개선	침해사고 대응절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다. 모의훈련 결과는 침해사고 대응절차에 반영하여 주기적으로 개선하여야 한다.	
	7.4.3 침해사고 대응	개인정보 침해사고 발생 시 절차에 따라 신속히 복구를 수행하고, 사고분석 후 발견된 취약점은 관련 조직 및 임직원과 공유하며, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여 침해사고 대응체계에 반영하여야 한다.	

용되는 접근권한, 접속기록, 접근통제, 운영보안, 암호통제는 해당되는 영역에 한해서만 준수할 필요가 있다. 또한 기술적인 부분은 수탁을 주는 경우가 많으므로 이에 대한 별도의 지침이 마련될 필요가 있다.

3.2.9 물리적 보호조치 항목

<표 10>은 물리적 보호조치에 대한 표이다. 물리적 보호조치의 필수 항목은 대부분 CCTV와 관련된 영상정보 처리기기 관리 및, 물리적 보안 관리, 매체관리의 영역으로 나뉘며 보호구역의 지정 및 관리의 부분에 한하여 세부적으로 보호구역지정, 보호설비, 보호구역 내 작업, 모바일 기기 반 출입 제한 등에 대한 내용을 추가하여 의료기간 시설 전반에 대한 환경적인 부분의 보안이 요구된다. 특히, 물리적 보안관리 부분 역시 정보구역에 대해 정보 절차와 운영에 대해

<표 9> 기술적 보호조치 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
기술적 보호조치	8.1.2 개인정보취급자 등록	개인정보 및 개인정보처리시스템의 접근을 통제하기 위한 개인정보취급자 등록 및 해지 절차를 마련하여야 한다. 또한, 개인정보 취급 PC의 보안책임이 자신에게 있음을 규정화하고 인식시켜야 한다.	필수
	8.1.3 개인정보취급자 권한관리	개인정보처리시스템의 접근권한은 최소한의 업무수행자에게만 부여하고 권한변경 내역을 보관하여야 한다.	필수
	8.1.4 특수권한 관리	개인정보 및 개인정보처리시스템에 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	필수
	8.1.5 개인정보취급자 접근권한 검토	개인정보 및 개인정보처리시스템 등을 사용하는 개인정보취급자의 접근권한 현황을 정기적으로 점검해야 한다.	
	8.1.6 개인정보취급자 인증 및 식별	개인정보처리시스템 접근 시 안전한 인증 절차에 따라 통제하고, 필요한 경우 법적요구사항 등을 고려하여 강화된 인증방식을 적용해야 한다.	필수
	8.1.7 비밀번호 관리	법적요구사항, 외부 위협요인 등을 고려하여 개인정보취급자 및 사용자, 정보주체(이용자)의 비밀번호 관리절차를 수립하고 이행하여야 한다.	필수
	8.2.1 개인정보처리시스템 접속기록 관리	개인정보처리시스템의 접속기록을 보관하고, 접속기록의 정확성을 보장하기 위해 관련 장비 및 시스템을 표준시간으로 동기화하여 해야 한다.	필수
	8.2.2 접속기록 모니터링	접속기록은 위·변조되지 않도록 보호대책을 적용하여야 하며, 개인정보의 오남용이 발생되지 않도록 모니터링을 수행하여야 한다. 또한 문제 발생 시 적절한 사후조치가 적시에 이루어져야 한다.	
	8.3.1 네트워크 접근	유·무선 네트워크에 대한 비인가 접근을 통제하기 위해 네트워크 접근통제 관리절차를 수립하고 서비스, 사용자 그룹, 개인정보 자산의 중요도, 법적요구사항에 따라 네트워크를 분리하여야 한다.	필수
		- 무선네트워크 물리적·관리적 보안 강화 - 안전한 무선 인증 및 암호화 적용 - 무선 IPS - 네트워크 접근제어	추가
	8.3.2 서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.	필수
	8.3.3 응용 프로그램 접근	사용자의 업무 또는 직무에 따라 개인정보를 취급하는 응용프로그램 접근권한을 제한하여야 한다.	필수
	8.3.4 데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립·이행하여야 한다.	필수
	8.3.5 원격 운영접근	내부 네트워크를 통하여 개인정보처리시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 외부 네트워크를 통하여 개인정보처리시스템을 관리하는 것은 원칙적으로 금지한다. 부득이한 사유로 인해 허용하는 경우에는 관련 법률에 따른 보호대책을 수립하여야 한다.	
	8.3.6 인터넷 접속 통제	개인정보처리시스템에 접근 가능한 개인정보취급자의 PC는 인터넷 접속 또는 서비스를 제한 및 통제하고, 필요시 인터넷 접속내역을 모니터링 하여야 한다.	
	8.4.3 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템과 개인정보취급자 단말기(PC, 노트북 등)를 보호하기 위해 보호대책을 수립하여야 한다.	필수
	8.4.4 취약점 점검	개인정보처리시스템에 대한 비인가 접근 시도 등을 예방하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.	
	8.4.5 개인정보 표시제한	개인정보 조회, 출력 등을 수행할 경우, 마스킹 기술 등을 통해 개인정보 표시를 제한하여야 한다.	
	8.4.6 보안 시스템 설치·운용	불법적인 접근 및 침해사고 방지를 위해 침입차단 및 탐지 기능을 포함한 시스템을 설치·운용하여야 한다. 또한, 보안시스템 운영절차를 수립하고 보안시스템별 정책적용 현황을 관리하여야 한다.	
	8.4.7 공개 서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.	필수
	8.4.8 모바일 기기 관리	업무 목적으로 모바일기기를 내·외부 네트워크에 연결하여 사용할 경우 모바일기기 접근통제 대책을 수립하여야 한다.	

	8.4.10 패치 관리	소프트웨어, 운영체제, 보안시스템 등에 대하여 시스템에 미치는 영향을 분석하여 주기적으로 최신 패치를 적용하여야 한다.	필수
	8.5.1 암호화 정책 수립	개인정보를 안전하게 관리하기 위하여 법적 요구사항을 반영한 암호화 정책을 수립하여야 한다.	
	8.5.2 암호화 적용	암호화 정책에 따라 개인정보 저장 및 전송, 원격접속 시 암호화를 수행하고 암호키를 안전하게 관리하여야 한다.	필수
		암호화대상 개인정보를 저장할 때 암호화를 적용하는 경우 - 개인정보의 저장 현황 - 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법 - 암호화 추진 일정 등이 포함된 “암호화계획”을 수립하여야 함	추가

<표 10> 물리적 보호조치 항목[25, 31-33]

통제분야	통제항목	상세내용	비고
물리적 보호조치	9.1.1 영상정보처리기기 설치·운영 제한	영상정보처리기기 설치·운영 시, 설치 목적에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호조치를 마련하여야 한다.	필수
	9.2.1 보호구역의 지정 및 관리	주요 설비 및 시스템을 보호하기 위하여 보호구역을 지정하고 보호구역 내의 작업 절차를 포함하여 보호대책을 수립·이행하여야 한다. 보호구역의 특성에 따라 보호설비를 갖추고 운영하여야 한다. 또한 외부 집적정보통신시설에 위탁·운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토하여야 한다.	
		세부항목 : 보후구역지정, 보호설비, 보호구역 내 작업, 출입통제, 모바일기기 반출입 제한의 내용을 추가	추가
	9.2.2 출입통제 및 사무실 보안	보호구역은 인가된 사람만이 접근할 수 있도록 통제하고 출입 및 접근 이력을 주기적으로 검토하여야 한다. 또한 사무실에서 공용으로 사용하는 사무용 기기 등에서 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.	필수
	9.2.3 개인업무 환경 보안	책상 위에 중요 문서나 저장매체를 남겨놓지 않고, 중요정보가 노출되지 않도록 보호대책을 수립·이행하여야 한다.	필수
	9.3.1 개인정보처리시스템 저장매체 관리	개인정보처리시스템 저장매체 관리절차를 수립하여 운영하고, 개인정보처리시스템 폐기 및 재사용 시 매체에 기록된 개인정보는 복구 불가능하도록 완전히 삭제하여야 한다.	필수
	9.3.2 휴대용 저장매체 관리	휴대용 저장매체를 통해 개인정보 유출이 발생하거나 악성코드가 감염되지 않도록 관리하고, 개인정보가 포함된 휴대용 저장매체는 안전한 장소에 보관하여야 한다.	
	9.3.3 이동 컴퓨팅 관리	보호구역 내 임직원 및 외부자의 이동 컴퓨팅에 대하여 반·출입을 통제하고 기록·관리하여야 한다.	

의료기관 종사자들에게 적용되는 범위 내에서 정책 및 보호 대책을 기반으로 하는 정보보호 조치가 필요하다.

Ⅳ. 설문결과

4.1 설문방법과 설문문항의 구성

본 연구는 기존의 개인정보보호 관리체계의 내용을 기반으로 의료기관 종사자들을 중심으로 개선되야 하는 부분을 파악하고 의료정보보호를 위한 현행 방안을 도출해 내기 위해 객관적인 설문을 실시하였다. 정의 및 측정항목을 정리한 것이다. <표 11>은 설문지에 대한 구성이다.

응답자의 특성과 개인정보보호관리체계에 대한 내용을 3부분으로 개인정보보호 관리체계, 생명주기 관리보장, 개인정보보호 보호조치로 3부분으로 구분하였고, 총 74개의 문항으로 개선안에 대한 적합성 여부를 측정하였다.

<표 11> 설문문항의 구성

설문구성	내용	문항 수	평가방법
응답자 특성	응답자의 병원규모	1개 문항	보기선택
	응답자 직업의 종류	1개 문항	보기선택
	응답자의 경력	1개 문항	보기선택
	정보보호교육 이수유무	1개 문항	보기선택
	개인정보보호관리 필요 유무	1개 문항	보기선택
개인정보보호 관리과정 단계	정책 및 범위/조직/개인정보식별/위험관리/체제검토/교정 및 개선/교육	15개 문항	Likert scale
생명주기 및 권리보장	개인정보 수집/이용 및 제공/보유/파기 시 보호조치/정보주체의 권리보장	19개 문항	Likert scale
개인정보보호대책	교육 및 훈련/취급자 관리/위탁업무 관리/침해사고 관리/접근권한 관리/ 접속기록관리 / 운영보안/암호화 통제/영상정보처리기기 관리/물리적 보안관리/매체관리/	40개 문항	Likert scale

<표 12> 표본의 기술적 특성

구 분	항 목	빈도(비율)
의료기관의 규모	일반 의원(외래환자를 대상으로 의료행위를 하는 의료기관)	5명(27.78 %)
	병원(30개 이상 병상)	2명(11.11 %)
	종합병원(최소 7개 이상의 진료과목 및 진료과목마다 전속하는 전문의)	4명(22.22 %)
	상급종합병원(20개 이상의 진료과목 및 진료과목마다 전속하는 전문의)	7명(38.89 %)
의료기관 종사자의 직업	의사	4명(22.22 %)
	간호사	5명(27.78 %)
	의료기사	3명(16.67 %)
	의무기록사	5명(27.78 %)
	기타	1명(5.56 %)
경력	3년 미만	6명(33.33 %)
	3년 이상 ~ 7년 미만	7명(38.89 %)
	7년 이상 ~ 10년 미만	1명(5.56 %)
	10년 이상	4명(22.22 %)
개인정보보호교육 이수 유무	예	11명(61.11 %)
	아니오	7명(38.89 %)
개인정보보호관리 필요 유무	예	18명(100.00 %)
	아니오	0명(0.00 %)

설문대상자는 의료기관에 소속된 종사자들을 대상으로 하여 설문기간은 2016년 5월 1일 ~ 2016년 6월 6일 까지 총 30명에게 전자우편 및 종이설문지 발송, 온라인 설문 방식을 통해 진행하였으며, 설문에 대한 변별력 수준을 높이기 위해 개인정보보호관리체계에 대한 자료를 설문자료에 포함하여 제공하였다. 이 가운데 18명이 응답하였다. 설문응답의 단순화를 위해 모든 측정항목에 단일 균형 리커트 5점 척도를 사용하였고 설문은 익명으로 실시되었다.

4.2 설문 결과분석

4.2.1 설문대상자의 기술적 특성

<표 12>는 자료 분석에 사용된 총 18개의 표본의 의료기관의 규모, 직업, 경력, 개인정보보호교육 이수 유무, 개인정보보호관리의 필요 유무에 대한 응답자의 특성을 보여준다.

의료기관 종사자가 근무하는 기관의 규모 분포는

상급종합명원이 7명(38.89%)로 가장 높았고, 일반의원이 5명(27.78%), 병원이 2명(11.11%), 종합명원이 4명(22.22%)으로 조사되었다. 직업의 종류로 간호사와 의무기록사가 5명(27.78%)로 같았고, 의사가 4명(22.22%), 의료기사가 3명(16.67%), 기타가 1명(5.56%)이다. 경력 분포는 3년 이상 ~ 7년 미만이 7명(38.89%)로 가장 많았고, 7년 이상 ~ 10년 미만이 1명(5.56%), 10년 이상이 4명(22.22%)이다. 개인정보보호 관리교육 유무를 묻는 질물에 예라고 응답한 응답자는 11명(61.11%)이였고, 아나오라고 응답한 응답자는

<표 13> 개인정보보호 관리과정에 관한 설문결과

세부질문	매우 부적절하다	부적절하다	보통이다	적합하다	매우 적합하다
정책수립	0 명	0 명	3 명	14 명	1 명
	0.00%	0.00%	16.67%	77.78%	5.56%
정책의 유지관리	0 명	0 명	3 명	11 명	4 명
	0.00%	0.00%	16.67%	61.11%	22.22%
범위설정	0 명	0 명	5 명	11 명	2 명
	0.00%	0.00%	27.78%	61.11%	11.11%
개인정보보호(관리) 책임자의 지정	0 명	1 명	4 명	9 명	4 명
	0.00%	5.56%	22.22%	50.00%	22.22%
조직의 구성	0 명	0 명	5 명	12 명	1 명
	0.00%	0.00%	27.78%	66.67%	5.56%
역할 및 책임	0 명	0 명	4 명	11 명	3 명
	0.00%	0.00%	22.22%	61.11%	16.67%
개인정보 식별	0 명	0 명	4 명	11 명	3 명
	0.00%	0.00%	22.22%	61.11%	16.67%
개인정보 흐름 파악	0 명	1 명	6 명	8 명	3 명
	0.00%	5.56%	33.33%	44.44%	16.67%
위험 식별 및 평가	0 명	0 명	5 명	10 명	3 명
	0.00%	0.00%	27.78%	55.56%	16.67%
이행계획 수립 및 보호대책 구현	0 명	0 명	6 명	10 명	2 명
	0.00%	0.00%	33.33%	55.56%	11.11%
내부감사	0 명	0 명	5 명	10 명	3 명
	0.00%	0.00%	27.78%	55.56%	16.67%
법적요구사항 준수검토	0 명	1 명	6 명	9 명	2 명
	0.00%	5.56%	33.33%	50.00%	11.11%
내부감사	0 명	0 명	2 명	13 명	3 명
	0.00%	0.00%	11.11%	72.22%	16.67%
개인정보보호 개선 활동	0 명	0 명	5 명	9 명	4 명
	0.00%	0.00%	27.78%	50.00%	22.22%
내부 공유 및 교육	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
평균	0.00%	1.19%	24.60%	57.14%	17.06%

7명(38.89%)으로 조사되었다. 개인정보보호관리가 필요하다고 생각한 응답자는 모든 응답자 18명(100%)으로 나타났다.

"매우 적합하다"와 "적합하다"라고 응답한 사람의 비율이 73.1%로 과반수이상으로 나타났으며, 설문결과는 아래의 <표13>과 같다.

4.2.3 생명주기와 권리보장에 관한 설문결과

생명주기와 권리보장에 대한 적합성 평가에 응답항목으로는 "매우 적합하다"와 "적합하다"라고 응답한 사람의 비율이 83.2%로 과반수이상으로 나타났으며, 설문결과는 아래의 <표14>과 같다.

<표 14> 개인정보보호 관리과정에 관한 설문결과

세부질문	매우 부적절하다	부적절하다	보통이다	적합하다	매우 적합하다
교육 및 훈련 시행·평가	0 명	1 명	4 명	9 명	4 명
	0.00%	5.56%	22.22%	50.00%	22.22%
개인정보 취급자 감독	0 명	0 명	5 명	9 명	4 명
	0.00%	0.00%	27.78%	50.00%	22.22%
보안서약서	0 명	0 명	3 명	11 명	4 명
	0.00%	0.00%	16.67%	61.11%	22.22%
퇴직 및 직무변경 관리	0 명	0 명	3 명	12 명	3 명
	0.00%	0.00%	16.67%	66.67%	16.67%
외부 위탁 계약	0 명	0 명	1 명	12 명	5 명
	0.00%	0.00%	5.56%	66.67%	27.78%
정보주체 고지	0 명	0 명	1 명	13 명	4 명
	0.00%	0.00%	5.56%	72.22%	22.22%
위탁자 관리·감독	0 명	1 명	1 명	12 명	4 명
	0.00%	5.56%	5.56%	66.67%	22.22%
침해사고 대응절차 및 체계구축-	0 명	0 명	3 명	13 명	2 명
	0.00%	0.00%	16.67%	72.22%	11.11%
침해사고 훈련 및 개선-	0 명	1 명	5 명	6 명	6 명
	0.00%	5.56%	27.78%	33.33%	33.33%
침해사고 대응	0 명	0 명	2 명	13 명	3 명
	0.00%	0.00%	11.11%	72.22%	16.67%
개인정보취급자 등록	0 명	0 명	3 명	12 명	3 명
	0.00%	0.00%	16.67%	66.67%	16.67%
개인정보취급자 권한관리	0 명	0 명	4 명	9 명	5 명
	0.00%	0.00%	22.22%	50.00%	27.78%
개인정보 수집 제한	0 명	0 명	5 명	8 명	5 명
	0.00%	0.00%	27.78%	44.44%	27.78%
정보주체의 동의	0 명	0 명	2 명	8 명	8 명
	0.00%	0.00%	11.11%	44.44%	44.44%
법정대리인 동의 및 고지	0 명	0 명	2 명	9 명	7 명
	0.00%	0.00%	11.11%	50.00%	38.89%

민감정보 및 고유 식별정보의 수집 제한	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
주민등록번호 수집·이용 제한	0 명	0 명	2 명	8 명	8 명
	0.00%	0.00%	11.11%	44.44%	44.44%
주민등록번호 대체수단	0 명	1 명	5 명	9 명	3 명
	0.00%	5.56%	27.78%	50.00%	16.67%
간접수집 보호조치	0 명	1 명	3 명	9 명	5 명
	0.00%	5.56%	16.67%	50.00%	27.78%
개인정보처리(취급)방침	0 명	0 명	5 명	9 명	4 명
	0.00%	0.00%	27.78%	50.00%	22.22%
개인정보 제3자 제공	0 명	0 명	2 명	11 명	5 명
	0.00%	0.00%	11.11%	61.11%	27.78%
제공받은 개인정보의 관리	0 명	0 명	3 명	5 명	10 명
	0.00%	0.00%	16.67%	27.78%	55.56%
개인정보 목적 외 이용 및 제공	0 명	0 명	2 명	9 명	7 명
	0.00%	0.00%	11.11%	50.00%	38.89%
개인정보의 이전	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
개인정보 품질 보장	0 명	0 명	2 명	9 명	7 명
	0.00%	0.00%	11.11%	50.00%	38.89%
개인정보 파기 규정 및 절차	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
개인정보의 파기	0 명	1 명	2 명	9 명	6 명
	0.00%	5.56%	11.11%	50.00%	33.33%
개인정보 열람	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
개인정보정정·삭제	0 명	0 명	2 명	8 명	8 명
	0.00%	0.00%	11.11%	44.44%	44.44%
개인정보 처리 정지	0 명	0 명	4 명	7 명	7 명
	0.00%	0.00%	22.22%	38.89%	38.89%
권리행사의 방법 및 절차	0 명	0 명	5 명	8 명	5 명
	0.00%	0.00%	27.78%	44.44%	27.78%
평균	0.00%	0.88%	15.79%	48.54%	34.79%

4.2.4 개인정보보호조치에 관한 설문결과

개인정보보호조치에 대한 적합성 평가에 응답항목으로는 “매우 적합하다”와 “적합하다”라고 응답한 사람의 비율이 80.4%로 과반수이상으로 나타났으며, 설문결과는 아래의 <표 15>과 같다.

Ⅴ. 결론과 향후 연구방향

6.1 결론

의료정보는 개인의 민감한 정보로써 이를 우선적으로 다루고 있는 의료기관의 정보보호의 관리체계와 요구사항에 대해 중요성이 강조되고 있다. 이러한

<표 15> 개인정보보호조치에 관한 설문결과

특수권한 관리	0 명	0 명	5 명	10 명	3 명
	0.00%	0.00%	27.78%	55.56%	16.67%
개인정보취급자 접근권한 검토	0 명	0 명	3 명	12 명	3 명
	0.00%	0.00%	16.67%	66.67%	16.67%
개인정보취급자 인증 및 식별	0 명	0 명	2 명	12 명	4 명
	0.00%	0.00%	11.11%	66.67%	22.22%
비밀번호 관리	0 명	0 명	3 명	11 명	4 명
	0.00%	0.00%	16.67%	61.11%	22.22%
개인정보처리시스템 접속기록 관리	0 명	0 명	3 명	13 명	2 명
	0.00%	0.00%	16.67%	72.22%	11.11%
접속기록 모니터링	0 명	0 명	4 명	10 명	4 명
	0.00%	0.00%	22.22%	55.56%	22.22%
네트워크 접근	0 명	0 명	5 명	11 명	2 명
	0.00%	0.00%	27.78%	61.11%	11.11%
서버 접근	0 명	1 명	2 명	13 명	2 명
	0.00%	5.56%	11.11%	72.22%	11.11%
응용 프로그램 접근	0 명	0 명	3 명	10 명	5 명
	0.00%	0.00%	16.67%	55.56%	27.78%
데이터 베이스 접근	0 명	0 명	6 명	10 명	2 명
	0.00%	0.00%	33.33%	55.56%	11.11%
원격 운영접근	0 명	0 명	4 명	11 명	3 명
	0.00%	0.00%	22.22%	61.11%	16.67%
인터넷 접속 통제	0 명	1 명	4 명	8 명	5 명
	0.00%	5.56%	22.22%	44.44%	27.78%
데이터베이스 접근	0 명	0 명	6 명	10 명	2 명
	0.00%	0.00%	33.33%	55.56%	11.11%
원격 운영접근	0 명	0 명	4 명	11 명	3 명
	0.00%	0.00%	22.22%	61.11%	16.67%
인터넷 접속 통제	0 명	1 명	4 명	8 명	5 명
	0.00%	5.56%	22.22%	44.44%	27.78%
개인정보 표시제한	0 명	0 명	4 명	8 명	6 명
	0.00%	0.00%	22.22%	44.44%	33.33%
보안 시스템 설치·운용	0 명	0 명	4 명	11 명	3 명
	0.00%	0.00%	22.22%	61.11%	16.67%
공개 서버 보안	0 명	0 명	3 명	9 명	6 명
	0.00%	0.00%	16.67%	50.00%	33.33%
모바일 기기 관리	0 명	0 명	4 명	7 명	7 명
	0.00%	0.00%	22.22%	38.89%	38.89%
패치 관리	0 명	0 명	3 명	11 명	4 명
	0.00%	0.00%	16.67%	61.11%	22.22%

암호화 정책 수립	0 명	0 명	4 명	9 명	5 명
	0.00%	0.00%	22.22%	50.00%	27.78%
암호화 적용	0 명	0 명	4 명	8 명	6 명
	0.00%	0.00%	22.22%	44.44%	33.33%
영상정보처리기기 설치·운영 제한	0 명	0 명	5 명	9 명	4 명
	0.00%	0.00%	27.78%	50.00%	22.22%
보호구역의 지정 및 관리	0 명	0 명	4 명	12 명	2 명
	0.00%	0.00%	22.22%	66.67%	11.11%
출입통제 및 사무실 보안	0 명	0 명	3 명	11 명	4 명
	0.00%	0.00%	16.67%	61.11%	22.22%
개인업무 환경보안	0 명	0 명	3 명	9 명	6 명
	0.00%	0.00%	16.67%	50.00%	33.33%
개인정보처리시스템 저장매체 관리	0 명	0 명	1 명	12 명	5 명
	0.00%	0.00%	5.56%	66.67%	27.78%
휴대용 저장매체 관리	0 명	0 명	2 명	10 명	6 명
	0.00%	0.00%	11.11%	55.56%	33.33%
평균	0.00%	0.70%	18.75%	57.36%	23.19%

발전하는 기술에 대해 의료기관에서 우선적으로 정보보호관리체계를 마련하기 위해 표준화된 정보보호 관리체계 구축이 필요하다.

본 연구는 의료정보의 특성을 고려한 개인정보보호관리체계를 이용하여 의료정보보호를 위한 개선안을 제안하였다. 이를 위해 기존의 개인정보보호관리체계의 항목에 대해 설문지를 기반으로 하여 행정자치부에서 발행한 의료부분의 개인정보보호가이드라인과 정보보호관리체계의 내용 및 기존 의료기관에 적용되던 정보보호와 관련된 선행연구의 내용을 반영하였다.

개정된 개인정보보호관리체계의 항목으로 구분하여 개인정보보호 관리과정, 개인정보보호 생명주기, 개인정보 보호조치의 내용을 기반으로 구성하였다. 본 연구는 의료정보보호를 위한 평가항목을 수집하고 활용하고 있는 의료기관 종사자들을 대상으로 설문조사를 실시하였다. 이를 통해 의료정보보호를 위해 의료기관 종사자들을 대상으로 개인정보보호 관리체계의 점검항목을 적용 하였으나 다음과 같은 한계점을 지니고 있다.

본 연구의 결과와 한계점을 요약하면 다음과 같다. 첫째, 개인정보보호 관리과정, 생명주기, 보호조치 항목이 효과적인 개인정보보호 관리체계의 점검 항목으로 적합한 것으로 확인 되었다. 이는 의료정보의 특성을 고려한 개인정보보호관리체계가 의료정보보호에도 적합한 것이다. 둘째, 의료기관의 종사자들을 대상으로 설문을 진행하여 의료기관 종사자가 다루기 어려운 부분인 기술적, 물리적 점검항목에 대해서는 문제 인식의 적합성을 판단하기에 다소 부족한 것으로 판단된다. 이는 의료정보를 다루는 의료기관 종사자를 대상으로 개인정보보호를 위한 보호조치에 대해 관리적 부분에 보다 초점을 두고 있기 때문이다. 이를 위해서 점검항목에 대한 교육과 의료정보보호 조치를 쉽게 이해할 수 있도록 개선안을 보안해야 한다. 셋째, 중소기업의 규모로 진행한 점검항목에 대해 소상공인 규모에 적용되는 필수적인 항목 이외 나

머지 항목은 소규모의 병원 규모에 따라 적용되기 어려운 부분이 있다. 기존의 개인정보보호 관리체계는 정보통신서비스 제공자를 위주로 작성되었기 때문에 의료기관에 적용되기 위해서는 의료기관의 상황을 고려하여 의료기관의 적용되는 개인정보보호점검항목을 개선하여 적용하기 위한 개선이 필요하다.

본 연구의 학문적, 실무적 시사점은 다음과 같다. 기존 의료정보를 위한 정보보호를 위한 연구 방법에 대해 기존 법률에서 규정하는 관리수준에 대한 연구가 주를 이루어 왔다. 하지만 본 연구에서는 개인정보보호 개선방법으로 최근 법 개정이 예정된 의료기관에 대한 내용을 따른 정보보호관리체계(ISMS)와 유사한 개인정보보호 관리체계(PIMS)를 통해 의료정보보호를 다루고 있다는 연구를 기반으로 하였다는 점에서 학문적 기여도가 크다고 할 수 있으며, 특히, 의료정보의 민감한 개인정보라는 특성을 고려하여 개인정보측면에서 개인정보보호 관리과정, 개인정보보호 생명주기, 개인정보보호조치 등 개인정보보호 관리체계를 기준으로 개선방안을 제안했다는 점에서 향후 연구에 기반이 되는 틀을 제공하였다. 실무적 시사점으로 의료기관 종사자들이 보다 의료정보를 다루는 전반적인 개인정보보호를 위한 세부적인 점검항목 및 개선내용을 통해 개인정보보호를 위한 전반적인 관리와 개선 항목을 보다 향상하여 크게 기여할 수 있을 것이다. 또한 개인정보보호 관리과정을 적용하여 체계적인 정보보호 대책을 수립하여 개인정보 사고를 미연에 방지 할 수 있을 것이다.

.

6.2 향후 연구방향

본 연구의 의의와 한계점, 추후 연구방향은 다음과 같다. 본 연구는 첫째, 의료정보를 다루는 의료기관 종사자들을 대상으로 하여 개인정보보호 관리체계의 개선 항목을 수립하였다. 하지만 자료의 수집에 있어서 의료기관 종사자들이 개인정보보호조치의 개선항목에 대한 기술적, 물리적 점검 항목에 있어서는 문항의 신뢰도를 판단하는데 한계가 있다. 또한 이러한 항목들의 경우 점검항목에 대해 의료기관의 경우 외부로 점검관리를 수탁하는 경우가 많아 이에 대한 점검항목의 전문성을 확보하기 위해서는 이와 관련한 수탁자들을 대상으로도 설문대상을 확대하여 개선항목에 대한 향후 연구를 진행할 필요성이 있다. 둘째, 본 연구에서는 중소기업과 소상공인 규모의 기업에서 적용 되는 인증항목을 기준으로 모든 의료기관에서 적용이 되는 적합한 개인정보보호 개선항목을 도출하였지만, 이는 모든 의료기관에서 적용하기 위한 공통의 기준으로 보기에는 병원의 규모나 현실적인 관리기반 부재 등 인증항목을 도출하는데 문제점이 있다. 이를 위해 의료기관에 적합한 개인정보보호 점검항목을 위해서는 의료정보보호 관리체계 구축에 대한 예산과 의료기관 종사자들의 정보보호 준수 교육 등 정보보호를 위한 지원이 필요하다. 마지막으로, 본 연구는 기존 개인정보보호법을 기반으로 하여 의료법에 대한 내용을 추가한 개인정보보호 관리체계에 대한 개선연구를 진행하였다. 하지만 의료기관을 대상으로 하기 위해서는 의료기관에 적용되는 의료법, 전자의무기록법, 정보통신망법 등 다른 법률에서 규정하는 내용에 대해서는 다루지 못하였다. 향후 연구에서는 이러한 법률에서 적용되는 각 법률에 적용되는 항목을 점검하고 통합하여 의료기관에 적합한 개인정보보호 관리체계의 개선항목 연구가 이루어져야 할 것이다.

참고문헌

[1] 정부균, “환자 의료정보 보호의 문제”, 의료법학, 제9권, 제2호, 2008, pp. 339-382.

[2] 보건복지부, “국가보건의료정보화 사업추진단 구성운영계획(안),” 2005.

[3] 이명길, “보건의료정보시스템 구축이 보건의료서비스에 미치는 영향 : 공공의료기관 중심으로,” 경희대학교 행정대학원 의료행정학과 석사학위논문, 2007.

[4] 이상영, “HL7/DICOM 게이트웨이를 활용한 병원정보시스템 구축,” 디지털산업정보학회 논문지 제6권, 제4호, 2010, pp. 1-10.

[5] 성수연, “의료정보의 공적활용과 개인정보보호,” 고려대학교 법무대학원 의료법학과 석사학위논문, 2009.

[6] 우성희, “IoT 환경의 의료 정보보호와 표준 기술,” 한국정보통신학회 논문지, 제19권, 제11호, 2015, pp. 2683-2688.

[7] 송화진, “지방의료원 정보보호 현황 분석을 통한 의료 정보보호 개선방안 연구,” 고려대학교 정보보호대학원 공공보안정책학과 석사학위논문, 2015.

[8] Identity Theft Resource Center, “Identity Theft Resource Center Breach Report Hits Record High in 2014,” 2014.

[9] OECD “Improving Health Sector Efficiency: The Role of Information and Communication Technologies,” OECD publishing, 2010, pp. 159.

[10] 최민경, “개인의료정보의 실질적 보호를 위한 법제 개선에 관한 연구,” 동국대학교 대학원 법학과 석사학위논문, 2015.

[11] 이근호, “개인의료정보 유출에 따른 민사책임,” 중앙대학교 대학원 법학과 석사학위논문, 2015.

[12] 윤성태, “모바일 의료정보 보안 구현 방안에 관한 연구 : ISO/TC 215 WG4 국제표준의 국내 허가 규정 적용을 중심으로,” 호서대학교 벤처대학원 융합공학과 석사학위논문, 2016.

[13] 신상열・양환석, “응급의료정보시스템의 보호를 위한 보안 구조,” 디지털산업정보학회 논문지, 제8권, 제2호, 2012, pp. 59-65.

[14] 김동명, “유비쿼터스 의료정보시스템을 위한 익명성 기반의 개인정보보호 기법,” 충북대학교 대학원 전자계산학과 박사학위논문, 2007.

[15] 박광희, “국내 치과 병・의원 정보화 현황과 정부지원 정책 방향에 관한 연구,” 연세대학교 보건대학원 보건정보관리학과 석사학위논문, 2006.

[16] 이재욱, “보건의료관광 활성화를 위한 정책 제언 연구,” 경희대학교 관광대학원 관광경영학과 석사학위논문, 2009.

[17] 양민희, “근거중심 보건의료 정책결정을 위한 연구분류체계 개발,” 고려대학교 보건대학원 보건정책및병원관리학과 석사학위논문, 2015.

[18] 김형기, “보험회사간 의료정보 공유제도,” 보험학회지, 제 65권, 2003, pp. 67-91.

[19] 백윤철, “헌법상 환자의 의료정보에 대한 권리에 관한 연구,” 헌법학연구, 제11권, 제3호, 2005, pp. 337-373.

[20] 이한주, “개인의료정보의 헌법적 보호,” 고려대학교 대학원 법학과 박사학위논문, 2011.

[21] 노문종, “의료 환경에서 XDS를 이용한 의료정보의 공유에 관한 연구,” 건국대학교 정보통신대학원 정보통신 e-business 석사학위논문, 2005.

[22] 염흥열, “개인정보보호 관리체계 국제 표준화 필요성,” 정보보호학회지, 제23권, 제4호, 2013, pp. 65-72.

[23] 전진환・조강래, “개정 고시에 따른 개인정보보호 관리체계(PIMS)인증의 주요변화,” 정보보호학회지, 제23권, 제5호, 2013, pp. 20-23.

[24] 박대하・한근희, “클라우드 서비스 환경의 개인정보 위탁을 위한 개인정보보호 관리체계,” 정보보호학회논문지, 제23권, 제6호, 2013, pp.

1267-1276.

[25] 한국인터넷진흥원, “PIMS 인증 운영절차 및 신청 안내,” 개인정보보호 관리체계 인증제도 설명회 자료, 2016.

[26] 한국인터넷진흥원, “PIMS 인증통합에 따른 제도 운영 방안,” 개인정보보호 관리체계 인증제도 설명회자료, 2016.

[27] 심미나, “효율적인 개인정보관리체계(PIMS) 인증제도 도입방안 연구 : 정보보호관리체계(ISMS) 인증제도와의 중복성 해소방안을 중심으로,” 고려대학교 정보경영공학전문대학원 정보경영공학과 박사학위논문, 2010.

[28] 채은지, “은행부문의 개인정보보호관리체계(PIMS) 기반 개인정보 유출방지 모니터링 방법론 연구,” 동국대학교 대학원 정보보호학과 석사학위논문, 2014.

[29] 차건상・한호현・신용태, “개인정보보호법의 자율규제 확보를 위한 효과적인 개인정보관리체계 인증제도,” 정보과학회논문지, 제39권, 제3호, 2012, pp. 276-281.

[30] 최희성, “의료정보보호를 위한 의료기관 종사자들의 인식과 태도,” 부산카톨릭대학교 생명과학대학원 병원경영학과 석사학위논문, 2010.

[31] 행정자치부, “의료기관 개인정보보호 가이드라인,” 2015. 2.

[32] 김소라, “중복성 평가를 통한 개인정보보호 관리체계 인증제도 개선방안,” 충북대학교 일반대학원 정보보호경영학과 석사학위논문, 2016.

[33] 이준화・조희준・박성갑・강윤철, “의료부분 정보보호 관리체계 개선방안 연구,” 한국정보보호학회지, 제 23권, 4호, 2013, pp. 34-40.

■ 저자소개 ■

민 경 은
Min Kyeongeun

2011년 2월 덕원여자 고등학교 졸업
2015년 2월 남서울대학교 치위생학과 졸업
2016년 6월 남서울대학교 복지경영대학원 산업보안학과 재학

관심분야 : 정보보호, 정보보안, 의료정보, 헬스케어, 빅데이터, 사물인터넷
E-mail : znf3znf@naver.com

김 성 준
Kim Seongjun

2003년 2월 동국대학교 법학과 졸업
2006년 8월 동국대학원 법학과 석사과정 졸업
2009년 2월 동국대학교 법학과 박사과정 대학원 졸업
2014년 2월 연세대학교 정보대학원 박사 수료
2014년2월 남서울대학원 대학원 산업보안학과 조교수

관심분야 : 개인정보, 개인정보보호법, 정보보호, 사물인터넷, 빅데이터
E-mail : mvstar@hanmail.net

논문접수일: 2016년 8월 20일
수 정 일: 2016년 9월 1일
게재확정일: 2016년 9월 7일