Korea Institute for Health and Social Affairs

연구보고서 2013-29

의료기관의 개인정보보호현황과 대책

정영철 · 이기호 · 이야리

KIHASA 한국보건사회연구원
Korea Institute for Health and Social Affairs

【책임연구자】
정영철 한국보건사회연구원(연구위원)

【주요저서】
보건복지 부문의 소셜미디어 활용현황 및 정책과제
한국보건사회연구원, 2012(공저)
온라인 및 모바일기반의 보건의료서비스 이용행태 및 활용에 관한 지표생산을 위한 기초연구
한국보건사회연구원, 2012(공저)

【공동연구진】
이기호 한국보건사회연구원 전문연구원
이아리 한국보건사회연구원 초빙연구위원

연구보고서 2013-29

의료기관의 개인정보보호현황과 대책

발 행 일 2013년
저 자 정 영 철 외
발 행 인 최 병 호
발 행 처 한국보건사회연구원
주 소 서울특별시 은평구 진흥로 235(우:122-705)
전 화 대표전화: 02)380-8000
홈페이지 http://www.kihasa.re.kr
등 록 1994년 7월 1일 (제8-142호)
인 쇄 처 경성문화사
가 격 7,000원

ISBN 978-89-6827-060-4 93510

발간사

1980년대 초 국가기간전산망사업을 시작으로 진행된 우리나라의 '정보화'는 2012년도 UN의 전자정부 발전지수 및 온라인참여지수, ITU의 ICT 발전지수 등에서 1위를 차지하며 정보화강국, 인터넷강국의 면모를 여실히 드러내고 있다. 이러한 '정보화', '정보통신기술'의 발전은 일상생활의 편리성, 국가경쟁력 강화 등과 같이 수많은 순기능적인 측면도 있지만 불법스팸, 해킹, 프라이버시 침해, 개인정보 오남용 등과 같은 역기능적인 측면도 지니고 있어 양면성을 띠고 있다.

정보화 역기능 중에서도 개인정보 유노출, 이로 인한 프라이버시 침해는 개인적, 사회적, 국가적으로 많은 폐해를 보이고 있어 세계 각국에서는 정부차원의 법제화, 자율규제적인 인증제도 시행 등을 시도하고 있다.

우리나라에서도 세계적 추세에 발맞추어 2011년 3월「개인정보 보호법」이 제정되고 같은 해 9월부터 시행되면서 사회적으로 개인정보 보호에 대한 많은 관심이 나타나고 있는 가운데, 민감한 개인의료정보가 수집, 보관, 이용되고 e-Health, u-Health 등과 같은 IT 기술발전에 의한 새로운 패러다임, 새로운 서비스들이 등장하고 있는 의료영역에서 의료기관을 중심으로 한 개인의료정보보호의 관리현황과 이에 대한 문제점, 그리고 대처방안을 마련해야 할 시점이라 할 수 있다.

이에 본 연구에서는 개인의료정보를 대부분 생산, 보관, 관리하고 있는 의료기관에서의 개인정보 보호 즉, 개인의료정보 보호에 대한 관리실태를 파악, 문제점 및 취약점들을 분석하여 이에 대한 정책적 대응방안을 마련하고자 하였다. 다만 직접 현장점검 혹은 대면을 통한 실태조사가 아

닌 설문지를 통한 온라인 조사를 실시함에 있어 관리실태에 대한 조사결과의 정확성이 일부 떨어질 우려도 있으나 이는 본 연구의 한계점으로 둔 채, 추후 의료기관에 대한 주기적인 실태조사를 기대코자 한다.

본 보고서는 정영철 연구위원의 책임 하에 이야리 초빙연구위원, 이기호 전문연구원에 의하여 작성되었으며 보고서의 완성도를 위하여 많은 조언을 준 보건복지부 정채용 과장, 가톨릭대학교 김석일 교수, 그리고 본 원의 최정수 연구위원, 윤강재 부연구위원에게 감사의 뜻을 전한다.

또한 본 연구에서의 설문조사를 위하여 많은 협조와 조언을 제공해 준 전국 시도 의사회 정보통신위원회 위원들, 대한병원협회, 대한중소병원협의회, 대한병원정보협회, 전국지방의료원연합회의 관계자 여러분, 그리고 건강정보광장, 금연길라잡이, 건강길라잡이 사이트 운영진 여러분들께 감사드리며 아울러 설문조사 수행, 결과 정리 및 분석에 도움을 준 전혜인 전문원, 조주현 전문원께도 감사드린다.

2013년 12월

한국보건사회연구원장

최 병 호

목 차

표 목차

그림 목차

Abstract

A Study on Current Privacy Policies of Medical Institutes and Suggestions

□ According to rapid development of information technology, mobility and accessibility to personal medical records have been on the rise in medical industry. At the same time, a risk of breach of personal medical information has gradually increased.

□ Therefore, this study has attempted to investigate how the sensitive personal health data which can cause a serious problem if breached have been managed in medical institutes, analyze the weakness and problems of the management and come up with decent policies.

□ For this, the following four surveys have been conducted; current management of personal medical records in medical clinics and medical doctors' awareness on the protection of personal medical information, control of personal medical records by the medical record manager in the medical clinic, current management of privacy policy through analysis on the website of the medical

clinic, the general public's awareness on the protection of personal medical records.

□ Then, the following results have been obtained:

○ In terms of awareness on five rights concerning Personal Information Protection Act-related personal information subjects, doctors (65.1%) were higher than the general public (57.7%).

○ Doctors believe that the public's interest in their medical records is 2.21 out of 5 scores.

○ In terms of importance of protection of personal information, the general public (4.25) were higher than doctors (4.06).

○ In terms of the control of personal medical information, doctors (2.94) were higher than the public (2.49).

○ In terms of disclosure of personal information policy, hospitals (81.0%) were higher than medical clinics (46.7%).

□ Based on these results, this study can be concluded as follows:

○ Recently, regulations on the protection of personal information have become more stringent. Therefore, it is necessary to develop a decent personal medical data

management plan with more interest in medical sectors. For this, it is required to investigate current situations on a regular basis.

○ Within the conventional self-regulatory personal information protection authentication system, it is needed to come up with evaluation criteria specialized for a medical sector. In addition, it's necessary to strengthen the assessment categories associated with the protection of personal medical information within the current authentication assessment system.

○ Furthermore, there should be more aggressive PR and education activities against the general public, medical workers (medical doctors, hospital employees) and employees of medical information system developers.

○ It is also required to develop customized education contents by type of medical institute, circumstance and duty and provide them systematically.

○ It is needed to deal with issues associated with the protection of personal medical records in health-related portals and mobile apps as well as in medical institutes and public organizations as well.

요 약

1. 연구배경 및 목적

□ 세계 각국에서 개인정보 보호를 위해 정부차원의 법제화를 추진하고 있는 가운데 우리나라에서도 2011년 3월 「개인정보 보호법」이 제정되면서 사회 각 분야에서의 개인정보 보호에 대한 관심이 계속 증가하고 있음.

□ 정보화에 따른 개인의료정보의 디지털화, 웹환경 확대, e-Health u-Health 등과 같은 IT 발전 등으로 인해 의료부문에서의 개인의료정보에 대한 접근성과 이동성이 증가되어 개인의료정보에 대한 침해, 유노출의 위험이 점점 더 커지고 있음.

□ 이에 정보특성상 가장 민감하고 침해시 심각한 피해가 예상되는 개인의료정보가 생성, 관리, 이용되고 있는 의료기관에서의 개인정보 보호 관리실태를 파악, 문제점 및 취약점들을 분석하여 이에 대한 정책적 대응방안을 마련하고자 함.

2. 주요 연구결과

□ '개인정보'는 살아 있는 개인에 관한 정보(개인정보 보호법 제2조)로 시대, 기술, 인식이 변화하면서 적용대상과 범위 또한 변화하게 됨.

□ ‘개인의료정보’는 의료기관을 중심으로 수집, 이용, 관리되는 개인정보로써, 일반적인 개인정보보다 정보주체와의 관련성이 크고, 침해시 그 피해가 더 크며, 정보 보호 뿐 아니라 적절한 이용 및 활용과의 균형도 중요한 과제가 되고 있음.

□ ‘개인건강정보’는 의료기관 뿐 아니라 공공기관, 관련 협·단체, 건강관련 포털, 모바일 앱 등을 통해 수집되고 이용·관리되는 건강을 유지하고 관리하는 데 필요한 포괄적인 정보로써 개인신상정보, 개인의료정보, 개인건강관리정보 모두 포함함.

□ ‘정보화역기능’은 정보화 진전에 따라 컴퓨터 및 인터넷등 정보통신수단을 이용하거나 정보통신수단에 대해 행하여지는 해킹, 바이러스 유포등 각종 컴퓨터범죄 및 기타 정보화에 수반하는 제반 문제점임(정보통신부, 1999).

□ ‘개인정보 침해’란 정보주체의 동의없이 즉, 정당하지 않은 절차에 의해 개인정보가 수집·이용·제3자에게 제공되는 일체의 피해임(한국정보보호진흥원·개인정보분쟁조정위원회, 2007).

□ ‘개인정보 유출’이란 정보주체의 개인정보에 대해 법령에 의하지 않고 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용하는 것임(표준 개인정보 보호지침 제26조).

□ ‘개인정보보호’란 개인정보 유출을 막기 위해 개인정보 관리체계 수립, 개인정보 처리단계별 기준·절차 준수 및 안전한 관리, 정보주체 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동임(개인정

보 보호 인증제 운영에 관한 규정 제2조).

□ 우리나라 개인정보 보호법, OECD 프라이버시 가이드라인, EU의 개인정보 보호 지침, 미국 HIPAA 의 프라이버시 규칙 등 관련 법·제도를 살펴보았을 때 그 내용과 효력, 적용범위가 점차 강화되고 확대되고 있으며 자국 내 뿐 아니라 국제적인 교류에 있어서도 상호 적용되고 있는 추세임.

□ 정보보호실태조사, 공공기관 개인정보보호 관리수준 진단, 개인정보보호 현장점검, 보건복지부 소속·산하기관에 대한 개인정보 보호 관리수준 현황조사 등 관련조사를 살펴본 결과 보건복지부문, 의료기관에 대한 개인정보보호 관리실태와 더불어 개인의료정보 보호에 대한 인식수준을 파악할 수 있는 주기적인 조사는 없는 실정임.

□ 개인정보 보호마크(ePRIVACY Mark), 인터넷사이트 안전마크(i-Safe Mark), 개인정보보호 관리체계 인증제도(PIMS, Personal Information Management System), 개인정보 영향평가 제도(PIA, Privacy Impact Assessment), 개인정보 보호수준 인증제도(PIPL, Personal Information Protection Level), 일본의 P 마크 제도, 그리고 우리나라의 의료기관 인증제도 등 관련 인증제도를 살펴본 결과 의료기관과 같이 특정 영역의 특성을 잘 반영할 수 있는 부문별 영역별 인증체계로의 정립이 매우 필요한 시점임.

□ 본 연구에서 실시한 의원급 의료기관의 개인(의료)정보보호 관리현황 및 개원의 의사들의 개인(의료)정보보호에 대한 인식조사, 병원급 개인(의료)정보보호 관리현황을 파악하기 위한 조사, 의료기관

홈페이지 개인정보처리방침 관리현황조사, 일반국민의 개인(의료) 정보보호 인식현황 조사의 내용 및 방법 등은 다음과 같음.

〈표 1〉 본 연구에서의 개인의료정보보호 관리현황 및 인식현황 조사 개요

조사내용	조사대상	조사방법	조사항목	협조기관
의원급 개인의료정보 보호 관리현황 및 의사 인식현황	의료인 (의원 원장)	온라인조사/ 오프라인조사	3개부문 총 40개 항목	전국 시도의사회 정보통신위원회
병원급 개인의료정보 보호 관리현황	병원 (개인정보보호 담당자)	〃	7개부문 총 40개 항목	대한병원협회, 대한중소병원협의회, 대한병원정보협회, 전국지방의료원연합회
의료기관 홈페이지 개인정보 처리방침 관리현황	심평원등록 의료기관 홈페이지 (상급종합병원, 종합병원, 병원, 의원)	홈페이지 분석	개인정보 처리방침 10개항목	-
일반국민 개인의료정보 보호 인식현황	일반국민	온라인조사	4개부문 총 15개 항목	건강길라잡이, 금연길라잡이, 건강정보광장등 건강포털 및 보사연 홈페이지

□ 의원급 개인(의료)정보보호 관리현황 및 의사의 인식현황 조사결과

○ 16개 시·도 의사회 정보통신위원회 임원진을 대상으로 2013년 9월 23일 ~ 2013년 10월 25일까지 약 1달가량 온라인 및 서면 설문조사를 실시하였으며 총 105명이 응답에 참여함.

○ 개인정보 보호법에 대한 의원 의사들의 인지정도에서 '어느정도 혹은 잘 알고 있는' 즉 보통이상 알고 있는 경우는 32.4% 이었으며 개인정보 보호법 관련한 정보취득원은 의료계(동료), 관련 협·

단체, 인터넷 검색 순으로 나타남.

○ 개인정보 보호법 관련하여 정보주체에 대한 5가지 권리에 대한 인지도는 평균 65.1%, 개인정보 수집·이용에 대한 정보주체(법정대리인 포함)의 5가지 유형의 동의사항에 대한 인지도는 평균 80.9%, 정보주체의 동의 필요시 4가지 고지 필요사항에 대한 인지도는 평균 96.4%를 나타냄.

○ 최근 1년 동안 개인정보 보호관련 교육 경험률은 8.5%로 매우 낮았으며, 교육을 받지 않은 이유는 충분한 정보 및 소개가 부족하여 45.8%, 시간을 내지 못하여 19.8%, 필요성을 못 느껴 18.8%, 적절한 교육내용을 찾지 못하여 15.6% 순으로 나타남.

○ 의사들이 생각하는 우리나라 일반국민의 개인의무기록정보에 대한 관심수준은 5점 만점에 평균 2.21점으로 보통보다 낮다고 생각하고 있는 것으로 나타남.

○ 의사들이 생각하는 개인정보보호 중요도는 5점 만점에 평균 4.06점으로 개인의무기록정보 4.28점, 공공기관에서의 개인건강관리정보 4.22점, 일반개인정보 4.04점, 건강포털에서의 개인건강관리정보 3.90점, 모바일 앱에서의 개인건강관리정보 3.90점 순으로 나타남.

○ 의사들은 현재 개인정보보호 관리수준에 대해 5점 만점에 평균 2.94점으로 본인 의원에서의 개인의무기록정보 보호 관리수준 3.38점, 병원에서의 개인의무기록정보 보호 관리수준 3.33점, 의원에서의 개인의무기록정보 보호 관리수준 3.15점, 일반개인정보 보호 관리수준 2.97점, 공공기관에서의 개인건강관리정보 보호 관리수준 2.83점, 건강포털에서의 개인건강관리정보 보호

관리수준 2.48점, 모바일 앱에서의 개인건강관리정보 보호 관리수준 2.46점 순으로 평가함.

○ 의원의 개인정보처리방침에 대한 공개율은 46.7%, 개인정보처리시스템에 대한 6가지 항목에 대한 수행률은 평균 20.5%, 8가지 보안조치사항에 대한 이행률은 평균 32.1%, 개인정보관리 규정 중 외부업무위탁 시 7가지 문서화 필요사항에 대한 정답률은 평균 45.2%, 6가지 위탁자 수행업무에 대한 정답률은 평균 50.8%를 나타내고 있음.

□ 병원급 개인(의료)정보보호 관리현황 조사결과

○ 병원을 대상으로 2013년 9월 27일부터 2013년 10월 25일까지 약 1달간 온라인 및 서면 설문조사를 실시하였으며, 총 105개 병원이 응답에 참여함.

○ 개인의료정보보호 관련 예산에 있어 상대적으로 단기간 효과를 보일 수 있고 적용이 용이한 HW, SW 도입에 대한 예산책정 비율이 컨설팅, 모니터링, 교육, 홍보 부문에 대한 예산책정비율보다 높게 나타남.

○ 병원에서의 개인정보보호 업무담당인력은 평균 1.7명, 책임자가 지정되어 있는 병원은 전체 중 88.6%로 나타남.

○ 개인정보관리 규정 중 외부업무위탁 시 7가지 문서화 필요사항에 대한 정답률은 평균 86.3%, 6가지 위탁자 수행업무에 대한 정답률은 평균 81.9%를 나타내고 있음.

○ 병원의 개인정보처리방침에 대한 공개율은 81.0%, 영상정보처리기기에 대한 설치·운영률은 90.5%로 나타남.

○ 홈페이지 회원가입시 수집항목은 이름 83.7%, 전화번호 76.9% , 이메일주소 72.1% , 주소 65.4% , 주민등록번호 33.7% 등이었으며 인증수단으로는 주민등록번호 32.7%, 아이핀 26.0%, 휴대폰인증 17.3%, 공인인증 12.5% , 신용카드인증 4.8%을 사용하고 있는 것으로 나타남.

○ 개인정보처리시스템에 대한 6가지 항목에 대한 수행률은 평균 59.5%로 나타났으며 보안조치 상황에서는 보안프로그램 설치 및 업데이트 항목의 이행정도가 92.4%로 가장 높은 반면, 바이오정보에 대한 암호화 이행정도는 13.3%로 가장 낮게 나타남.

○ 병원 개인정보보호업무 담당자들은 우리나라 의료기관의 개인정보보호 관리수준은 5점 만점에 평균 2.66점, 본인 병원의 개인정보보호 관리수준은 평균 2.98점으로 그리 높지 않은 것으로 생각하고 있음.

□ 의료기관 홈페이지 개인정보처리방침 관리현황 조사결과

○ 건강보험심사평가원에 등록되어 있는 약 30,000여 의료기관을 대상으로 2013년 8월 1일부터 2013년 10월 18일까지 약 2달 반동안 인터넷 검색을 통해 분석함.

○ 분석결과, 홈페이지를 개설·운영하고 있는 기관은 과반수(50.9%) 정도이며, 이들 중 홈페이지에 개인정보 처리방침을 게재하고 있는 경우는 홈페이지 운영기관 중 51.4%에 그치고 있음[1].

1) 개인정보 처리방침은 홈페이지 뿐 아니라 사무소등 장소에 게시, 간행물, 관보 등에 게재

○ 필수기재 10개 항목에 대한 게시여부 및 내용의 충분성 분석결과 처리목적(98.4%), 처리항목(97.0%)에 대한 게시율이 높았으며 권리 및 의무사항(36,2%), 보호책임자사항(23.0%)에 대한 게시율이 낮았음. 또한 내용에 있어서는 특히 보호책임자사항과 권리 및 의무사항에 대한 내용이 충분하지 못한 것으로 나타남.

□ 일반국민의 개인(의료)정보보호 인식현황 조사결과

○ 건강관련 포털 3개(건강정보광장, 금연길라잡이, 건강길라잡이) 및 본 연구원 홈페이지 이용자를 대상으로 2013년 9월 27일 ~ 2013년 10월 10일까지 14일간 온라인 설문조사를 실시하여 2,730건을 최종 분석 자료로 사용함.

○ 개인정보 보호법에 대해 일반국민들은 '어느정도 혹은 잘 알고 있는' 즉 보통이상 알고 있는 경우가 16.4% 에 불과하였으며 개인정보 보호법 관련하여 정보주체에 대한 5가지 권리에 대한 인지정도는 평균 57.7%를 나타냄.

○ 일반국민이 생각하는 개인정보보호 중요도는 5점 만점에 평균 4.25점으로 일반개인정보 4.42점, 개인의무기록정보 4.32점, 공공기관에서의 개인건강관리정보 4.29점, 건강포털에서의 개인건강관리정보 4.17점, 모바일 앱에서의 개인건강관리정보 4.07점 순으로 나타남.

○ 일반국민들은 현재 개인정보보호 관리수준에 대해 5점 만점에 평균 2.49점으로 보통보다 낮게 평가하고 있었으며 공공기관에서

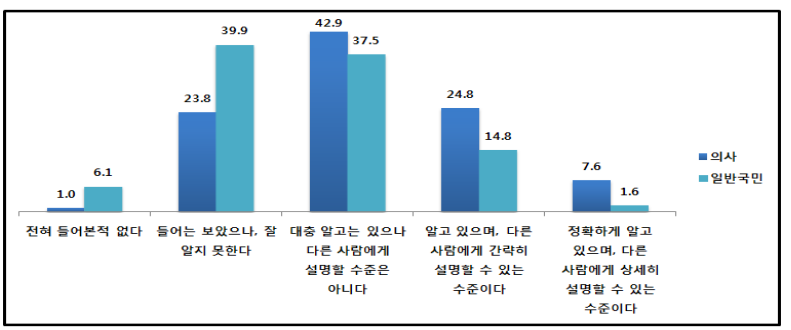
하는 등의 방법을 통해 공개할 수 있으므로 실제 개인정보 처리방침을 수립하여 공개하는 기관은 더 많을 것으로 예측할 수 있음.

의 개인건강관리정보 보호 관리수준 2.70점, 병원에서의 개인의무기록정보 보호 관리수준 2.55점, 의원에서의 개인의무기록정보 보호 관리수준 2.48점, 건강포털에서의 개인건강관리정보 보호 관리수준 2.47점, 모바일 앱에서의 개인건강관리정보 보호 관리수준 2.41점, 일반개인정보 보호 관리수준 2.31점 순으로 평가하여 공공기관에서의 관리수준을 가장 높게 평가함.

□ 의사 vs. 일반국민, 의원 vs. 병원 조사결과 비교

○ 개인정보 보호법에 대한 인지정도는 일반국민보다는 의사군이 더 높게 나타남.

〔그림 1〕 개인정보 보호법에 대한 인지정도

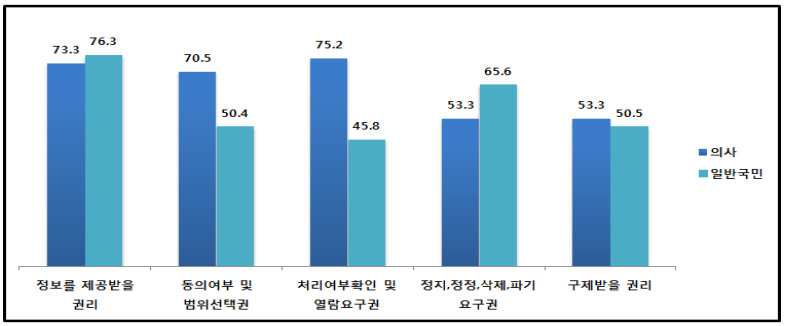


○ 홈페이지 운영에 있어 의원과 병원 모두 외부에 위탁하는 경우가 많게 나타남(의원의 경우 순수위탁 및 병행위탁 73.1%, 병원의 경우 순수위탁 및 병행위탁 78.2%).

○ 정보주체의 권리에 있어 동의여부 및 범위선택권, 처리여부 확인 및 열람요구권, 구제받을 권리에서는 일반국민보다는 의사군에서 인지정도가 더 높게 나타났으며 정보제공받을 권리, 정지·정정

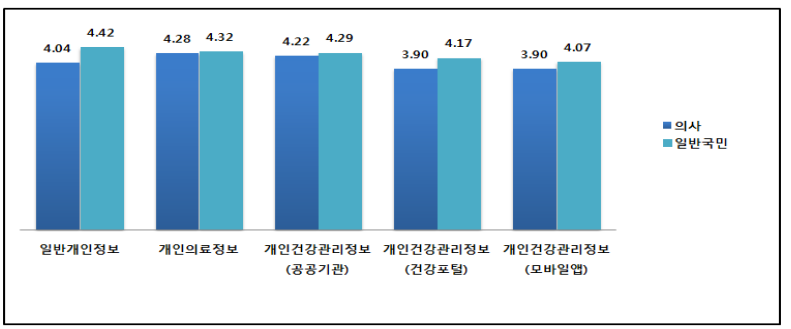
·삭제·파기 요구권에 대해서는 의사군보다 일반국민의 인지정도가 더 높게 나타남.

〔그림 2〕 정보주체권리에 대한 인지정도



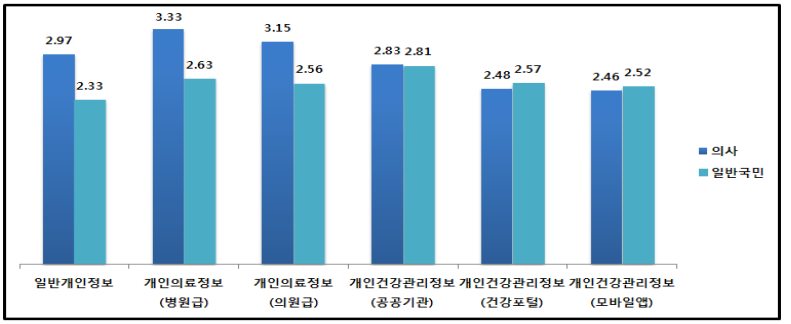
○ 개인정보 중요도에 대해 의사군보다 일반국민들이 더 중요하게 생각하고 있는 것으로 나타남.

〔그림 3〕 개인정보 중요도에 대한 인지정도



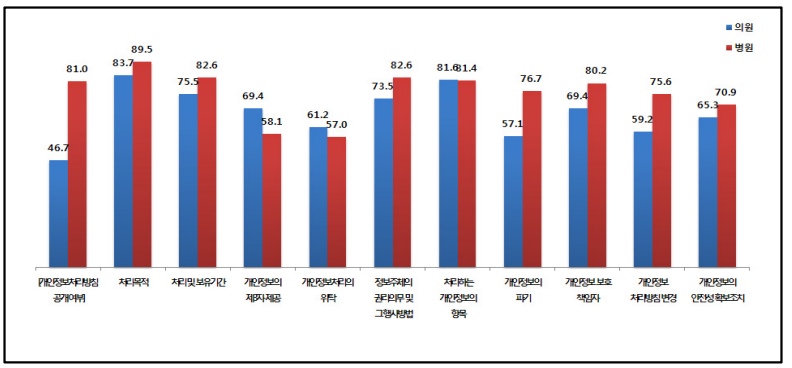
○ 개인정보 관리수준에 있어서는 의사군, 일반국민 모두 중요도에 비해 관리수준이 낮다고 평가하고 있음.

〔그림 4〕 개인정보 관리수준에 대한 인지정도



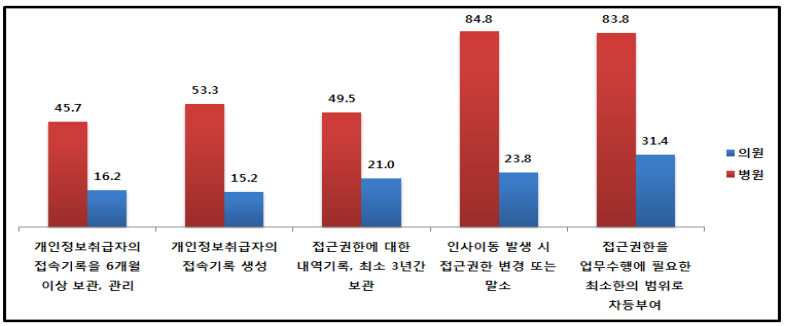
○ 개인정보처리방침에 대한 공개 및 개별항목에 대한 공개 여부에서는 병원급이 81.0%임에 비해 의원급은 46.7%로 상대적으로 공개정도가 낮음.

〔그림 5〕 개인정보처리방침 개별항목에 대한 공개여부



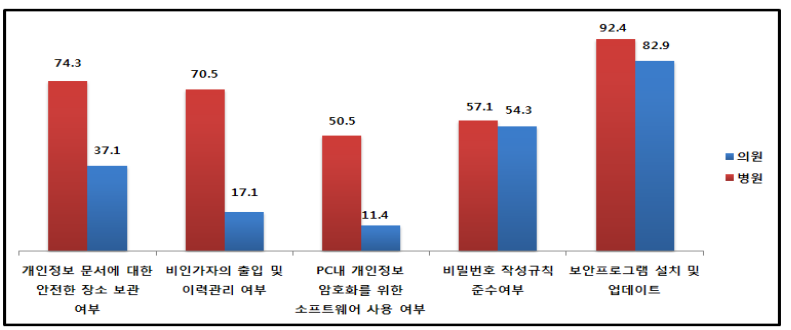
○ 개인정보 안전성 확보조치 수행현황에서는 의원급에서의 조치가 병원급보다 상대적으로 매우 낮은 것으로 나타남.

〔그림 6〕 개인정보 안전성 확보조치 수행현황



○ 보안조치 상황에서도 병원급이 상대적으로 의원급보다 많이 이행하고 있는 것으로 나타남.

〔그림 7〕 보안조치 현황



○ 의원급, 병원급 모두 정부에게 바라는 점으로는 보다 의료현실과 의료현장에 적합한 완화된 규제 적용, 체계적인 교육 실시, 상세한 가이드라인 제공, 인력지원과 예산 투자, 그리고 주민번호 대체방안 강구 등을 제시하고 있음.

□ 본 연구의 한계점은, 개인정보보호 관리현황 및 인식조사를 수행함에 있어 온라인 및 서면 설문조사 수행으로 인한 정확성 결여, 의원급 응답자 중 많은 수가 시도 의사회 정보통신위원회 임원진으로 인한 대표성 결여 등을 우려할 수 있음.

□ 의료기관의 개인의료정보보호 관리현황 파악에 있어 현장점검 혹은 대면을 통한 실태조사가 아닌 설문지를 통한 온라인 조사 혹은 서면조사를 실시함으로써 조사결과의 정확성이 일부 떨어질 우려가 있으며 응답 의원 및 병원급 의료기관의 대표성이 부족할 수 있음.

3. 결론 및 시사점

□ 의료기관의 개인의료정보 보호 수준향상을 위한 다양한 정책연구와 정책개발이 가능한 과제발굴에 있어 정부의 뒷받침이 필요함.

□ 정부 및 공공기관이 주도하여 의료기관 종류별 개인정보보호 관리현황 혹은 개인의료정보 보호, 개인건강정보 보호에 대한 인식을 주기적으로 파악하여 통계자료를 제공할 수 있는 실태조사 마련이 필요함.

□ 의료기관 종류별 맞춤형 필수 관리지침 혹은 교육콘텐츠 개발이 필요하며, 개발된 관리지침 및 교육콘텐츠 등을 체계적이고 명확한 안내를 수반한 보급을 위하여 보건복지부문 개인정보보호 창구가 필요함.

□ 정부 및 공공기관이 주도하여 의료기관 특성에 맞는 문제점 진단 및

기술지원 등 맞춤형 컨설팅을 제공할 필요가 있음.

□ 관련 협·단체 등과의 협의체 구성을 통하여 의료부문 개인정보 보호 전문교육 수행 및 인력양성을 위한 교육체계를 마련하고 분야별, 영역별 전문교육을 실시할 필요가 있음.

□ 의료영역에서의 개인정보보호 규제준수를 관리·감독하고 다양한 정책연구 및 정책개발, 주기적인 실태파악, 맞춤형 관리지침 및 교육콘텐츠 개발·보급, 맞춤형 컨설팅 제공, 교육체계 마련 등을 위해 보건복지분야의 별도 전문기관 육성이 필요함. 이러한 전문기관에 대한 필요요소로는 신뢰성, 전문성, 중립성 및 객관성, 인프라의 안정성, 업무의 지속성 등을 제시할 수 있음.

*주요용어: 의료기관, 개인의료정보보호, 보건복지분야 개인정보보호 전문기관

제1장 서 론

제1절 연구배경 및 목적

제2절 연구내용 및 방법

1 서 론

제1절 연구배경 및 목적

'정보(information)'라는 단어는 관측, 측정 등을 통해 수집된 자료를 실제 문제에 도움이 될 수 있도록 해석하고 정리한 지식이라 정의하고 있으며 이러한 단어를 우리나라에서 본격적으로 사용하기 시작한 것은 1960년대 이후이다[2]. 한편 이러한 정보를 생산·유통 또는 활용하여 사회 각 분야 활동을 가능하게 하거나 그러한 활동의 효율화를 도모하는 것을 '정보화'라 하였을 때[3], 산업사회에 이어 정보화가 주를 이루는 '정보화사회', 즉 정보가 사회적으로 중요하고 경제활동의 중심이 된 사회로 진입하게 되면서 정보와 지식은 국가 경쟁력의 원천이 되어 선진 각국에서는 경쟁적으로 정보화기반 구축을 위한 노력을 기울이게 되었다. 우리나라에서도 1980년대 초 국가기간전산망사업을 시작으로 정보화가 급속도로 진행되었으며 보건복지부문에서도 1990년대 중반 '국민복지망 기본계획'에서부터 적극적으로 추진되기 시작하였다(정영철외, 2003).

우리나라는 국가정보화기반을 근간으로 하여 정보화강국, 인터넷강국으로써 나날이 정보기술이 발전하고 있는 바, 인터넷이용실태조사 결과에 의하면 2012년도 만3세이상 인터넷이용률은 78.4%로 계속 증가하고

2) 한국브리태니커 온라인, http://preview.britannica.co.kr/bol/topic.asp?article_id=b19j1134b,[인용 2013.10.20.].; 한국민족문화대백과, http://terms.naver.com/entry.nhn?docId=547151&cid=1642&categoryId=1642, [인용 2013.10.20.].

3) 국가정보화기본법 제3조(정의).

있고(방송통신위원회·한국인터넷진흥원 2012a), 2012년도 UN의 전자정부 발전지수 및 온라인참여지수 1위, ITU(국제전기통신연합, International Telecommunication Union)의 ICT 발전지수 1위[4] 등 각종 정보화지수를 통해 그 면모를 여실히 드러내고 있다.

그러나 이러한 '정보화', '정보통신기술'의 발전은 우리 일상생활의 편리하고도 필요한 기능과 도구로 활용되는 동시에 국가 경쟁력의 하나로 인식되는 순기능적인 측면도 있지만 불법스팸, 해킹, 프라이버시 침해, 개인정보 오남용 등과 같은 역기능적인 측면도 지니고 있어 양면성을 띠고 있다 할 수 있다.

한편 '정보화', '정보통신기술'에 대한 활용이 점차 확대됨에 따라 개인정보가 전자매체에 대량으로 수집·축적되고 신속한 유통, 가공, 활용이 가능해지는 등 개인정보취급업무가 점점 확대되어 가면서 정보화 역기능 중에서도 개인정보 유출사고가 빈번하게 발생하고 있으며 이로인한 프라이버시 침해문제가 발생하는 등 개인정보 보호문제에 대한 사회적 불안감과 관심이 증폭하게 되었다(김태한, 2003).

우리나라 일반 국민들 중 64.5%가 인터넷으로 인해 개인정보 혹은 금융정보 등 유출이 걱정된다고 하였으며 이로 인한 명의도용, 개인신상정보 오남용과 같은 사회문제를 우려하고 있다(방송통신위원회·한국인터넷진흥원 2012a).

이에 세계 각국에서 개인정보 보호를 위해 정부차원에서 적극적으로 추진하고 있는 노력 중 하나가 법제화로써 우리나라에서도 2011년 3월 「개인정보 보호법」이 제정되어 같은 해 9월부터 시행되면서 사회 각 분야에서의 개인정보 보호에 대한 관심은 계속 증가하고 있다. 특히 개인정보

4) 한국정보화진흥원 사이트 중 '국제 정보화 지수현황', http://www.nia.or.kr/Contents/01_data/infostats.asp?BoardID=20111207155055 0012&order=010501, [인용 2013.06.19.].

침해 시 국가, 사회, 개인적으로 많은 경제적 피해가 예상되는 금융, 유통 분야와 더불어 민감한 개인의료정보를 다루고 있는 의료분야는 개인정보 보호 수준제고를 위해 국가차원의 종합적이고도 체계적인 노력이 요구되는 분야라 할 수 있다. 의료정보, 그 중에서도 개인을 식별할 수 있는 개인의료정보는 환자의 질병 및 치료와 관련된 개인정보로 대부분 의료기관에서 생산, 보관, 관리되고 있으며 정보특성상 가장 민감하고 보호가 필요한 부문이라 할 수 있다.

이러한 의료정보, 개인의료정보는 환자 진료 및 치료, 처방, 관련연구, 법률적 자료(소송에 따른 증거자료) 제출, 의료비 청구 등 의료기관 내/외부적으로 다양하게 사용되고 있으며 손실 혹은 파손이 발생하면 환자안전에 위험이 발생하고, 권한이 없는 자의 접근이나 정보유출은 윤리적인 문제 뿐 아니라 해당 의료기관에 대한 평판저하와 대중적 신뢰도 하락 등의 위험이 발생한다(정영철외, 2005).

한편 개인의료정보를 대부분 생산, 보관, 관리하고 있는 의료기관의 정보화는 1977년 의료보험 제도 시작 시 진료비 청구수단으로 활용된 이후 점차 전자의무기록(EMR), 처방전달시스템(OCS), 의료영상저장전송시스템(PACS) 등 각종 정보시스템이 도입되고 이러한 정보시스템에 의존하는 비중이 높아지게 되었다.

정보화로 인해 디지털화된 개인의료정보가 폭발적으로 생성되고 대규모 데이터베이스로 집적·통합되어 보안위협이 커졌으며 인터넷 등 웹환경 확대에 따른 병원환경이 개방되면서 정보보호에 대한 위협요소가 더욱 더 증가하게 되었다. 더우기 e-Health, u-Health 등과 같은 IT 기술발전에 의한 새로운 패러다임, 새로운 서비스들이 등장하면서 의료환경에서의 개인정보 유출로 인한 폐해는 더욱 더 복잡하고 다양한 문제를 야기할 가능성을 지니게 된 것이다(이유지, 2005; 한국정보보호진흥원, 2006).

이렇듯 개인의료정보 보호의 필요성과 중요성이 부각된 가운데 의료기관 및 의료기관 내 종사인력들의 보안의식이 부족하고 정보보호시스템 구축실태가 매우 미미한 수준이며 특히 공공이나 금융부문과 같은 타 산업분야에 비해 의료부문의 개인정보보호 수준 제고가 절실히 요구될 뿐 아니라(김동수·김민수, 2006; 조혜경, 2008) 개인정보 보호법 이후에도 그 이행정도가 저조하게 나타나고(엄현호, 2013) 있는 현실에 본 연구의 문제의식이 자리하고 있다.

그러므로 본 연구의 목적은 정보특성상 가장 민감하고 침해시 심각한 피해가 예상되어 보다 관심있는 보호가 필요한 개인의료정보를 대부분 생산, 보관, 관리하고 있는 의료기관에 대해 개인정보 보호에 대한 관리실태를 파악, 문제점 및 취약점들을 분석하여 이에 대한 정책적 대응방안을 마련하고자 하는 것으로 세부목적은 다음과 같다.

첫째, 국내 의료기관의 개인의료정보 보호관리 현황 및 문제점을 파악한다.

둘째, 개인의료정보 보호, 개인건강정보 보호에 대한 의료인 및 일반국민의 인식수준을 파악한다.

셋째, 국내 의료기관의 개인의료정보 보호관리 현황 및 문제점, 인식수준에 기반하여 개인의료정보 보호 관리기준 및 관리체계 구축을 위한 정책방안을 마련하고자 한다.

제2절 연구내용 및 방법

본 연구는 앞절에서 제시한 연구목적을 달성하기 위하여 총 5개의 장으로 구성하여 전개하고자 한다.

제1장 ‘서론’에서는 기존 문헌분석을 바탕으로 하여 의료기관에서의 개인정보보호, 즉 개인의료정보보호가 중요하며 수준제고가 필요한 배경과 본 연구의 목적을 기술하였으며 아울러 이를 위해 본 보고서를 구성하고 있는 연구내용과 방법을 제시하였다.

제2장 ‘이론적 배경’에서는 기존 문헌 및 미디어 기사 등을 고찰·분석하여 개인정보, 개인의료정보, 개인건강정보, 개인정보보호, 정보화역기능, 개인정보침해, 정보보호 및 개인정보보호 등에 관한 개념과 특징, 그리고 이들에 대한 우리나라 현황을 살펴보았으며 의료정보화 현황, 개인의료정보보호의 중요성과 필요성에 대해 다시한번 정리하였다.

제3장 ‘의료부문 개인정보보호관련 정책현황’에서는 관련 법·제도, 관련현황조사, 관련인증제도 등 크게 세 부문으로 나누어 정리하였다. 먼저 제1절 관련 법·제도에서는 기존 문헌분석, 관련 법률 및 고시등 분석을 통해 우리나라의 개인정보 보호법, OECD 프라이버시 가이드라인, EU 개인정보 보호지침, 미국 HIPAA 프라이버시 규칙등과 같은 개인정보보호 및 개인의료정보보호에 관한 대표적인 법·제도 내용을 간략하게 정리하였으며, 우리나라 개인정보 보호법에 따른 개인정보의 안전성 확보조치 기준, 표준 개인정보 보호지침, 보건복지부 개인정보보호 기본지침 등과 같은 관련제도에 관한 내용을 간단하게 정리하였다. 다음으로 제2절 관련현황조사에서는 기존 문헌분석, 보건복지부 및 안전행정부 내부자료 분석을 통해 기업 및 개인을 대상으로 한 정보보호실태조사, 안전행정부가 실시하고 있는 공공기관 개인정보보호 관리수준 진단과 개인정보보호 현장점검, 그리고 보건복지부가 실시하고 있는 소속·산하기관에 대한 개인정보보호 관리수준 현황조사 등에 관한 내용을 정리하였다. 마지막으로 제3절 관련 인증제도에서는 기존 문헌분석, 관련 법률 및 고시 등 분석, 관련사이트 분석, 해외사례분석 등을 통해 개인정보보

호마크(ePRIVICY Mark)와 인터넷사이트안전마크(i-Safe Mark) 같은 홈페이지 개인정보보호 인증마크제도, 개인정보보호 관리체계 인증제도(PIMS), 개인정보 영향평가제도(PIA), 개인정보 보호수준 인증제도(PIPL), 일본의 P마크제도, 그리고 우리나라의 의료기관 인증제도에 대해 간략하게 정리하였다.

제4장 '국내 의료기관의 개인정보보호 관리현황 및 개인의료정보보호에 대한 인식현황'에서는 제3장에서의 관련 현황조사 분석결과와 관련법률 및 고시등 분석, 공무원/관련 협단체/학계/연구원 등과 같은 관계자 정책간담회의 등을 통해 의원급 개인의료정보보호 관리현황과 의사의 인식현황, 병원급 개인의료정보보호 관리현황, 의료기관 홈페이지 개인정보처리방침 관리현황, 일반국민의 개인의료정보보호 인식현황을 파악하기 위한 조사설계를 수행하였으며, 이에 따라 의료기관 홈페이지 분석, 온라인 및 서면 설문조사 실시, 그리고 SPSS 통계분석을 통해 조사결과를 정리하였다.

의원급 개인의료정보보호 관리현황과 의사의 인식현황을 파악하기 위하여 개인정보 보호법, 개인정보 보호법 시행령, 개인정보의 안전성확보조치 기준을 근거로 응답자 및 의료기관 특성, 개인정보보호에 대한 인지정도, 개인정보보호 관리현황 등 3개부문 총 40개항목으로 조사표를 설계하였다. 조사는 전국 시도의사회 정보통신위원회 협조 하에 임원진 및 해당지역 의원을 대상으로 온라인 및 서면 조사표를 이용한 설문조사를 실시하였으며 조사결과는 SPSS 21 통계프로그램을 통해 빈도분석, 교차분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하여 정리하였다.

병원급 개인의료정보보호 관리현황을 파악하기 위하여 개인정보 보호법, 개인정보 보호법 시행령, 개인정보의 안전성확보조치 기준을 근거로

병원의 일반적 특성, 개인정보 보호 관리체계 구축, 개인정보 보호 대책 수립 및 시행, 침해사고 대책 개인정보 처리, 안전성 확보조치, 개인정보 보호 업무수행 등 7개부문 총 40개항목으로 조사표를 설계하였다. 조사는 대한병원협회, 대한중소병원협의회, 대한병원정보협회, 전국지방의료원연합회 등의 협조를 통해 온라인 및 서면 조사표를 이용한 설문조사를 실시하였으며 조사결과는 SPSS 21 통계프로그램을 통해 빈도분석, 교차분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하여 정리하였다.

의료기관 홈페이지 개인정보처리방침 관리현황을 파악하기 위하여 2013년 6월 현재 건강보험심사평가원에 등록·공개되어 있는 전국 의료기관 중 상급종합병원, 종합병원, 병원, 의원 약 30,000여 의료기관에 대해 홈페이지를 일일이 검색하였으며 개인정보처리방침 게재여부, 10개 필수 공개항목 각각에 대한 공개여부를 조사하여 빈도분석하였다.

마지막으로 일반국민의 개인의료정보보호 인식현황을 파악하기 위하여 개인정보 보호법을 근거로 응답자 특성, 의료기관 이용특성, 개인의료정보보호에 대한 관심, 개인정보보호에 대한 인식, 4개부문 총 15개항목으로 조사표를 설계하였다. 조사는 3개의 건강관련 포털(건강정보광장, 금연길라잡이, 건강길라잡이)과 본 연구원 홈페이지 이용자를 대상으로 온라인 설문조사를 실시하였으며. 조사결과는 SPSS 21 통계프로그램을 통해 빈도분석, 교차분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하여 정리하였다.

제5장 '결론 및 정책적 제언'에서는 앞 장에서 분석한 각종 제도 및 관리현황을 기반으로 관계자 정책간담회의를 거쳐 결론 및 의료기관의 개인정보 보호 수준향상을 제고하기 위한 정책방안을 제시하였다.

이상과 같은 본 연구의 내용 및 방법을 정리하면 〈표 1-1〉과 같다.

〈표 1-1〉 본 연구의 내용 및 방법

구분	연구내용	연구방법
제1장	배경 및 필요성 내용 및 방법	기존 문헌분석
제2장	개념 및 특성 의료정보화와 개인의료정보보호	기존 문헌분석 언론기사 분석
제3장	관련 법·제도 관련 현황조사 관련 인증제도	기존 문헌분석 관련 법률, 고시 등 분석 관련 사이트분석 보건복지부 및 안전행정부 내부자료분석 해외사례분석
제4장	조사설계 조사실시 및 조사결과 분석	관련 법률, 고시 등 분석 관계자 정책간담회의 온라인 및 서면 설문조사 의료기관 홈페이지 분석 SPSS 통계분석
제5장	결론 정책제언	관계자 정책간담회의

제2장 이론적 배경

제1절 개념 및 특성

제2절 의료정보화와 개인의료정보보호

2 이론적 배경

제2장에서는 본 연구의 문제의식에서 중심을 이루고 있는 개인정보, 개인의료정보, 개인건강정보, 정보화 역기능과 개인정보침해, 정보보호와 개인정보보호에 대한 개념과 특성 및 우리나라 현황에 대해 살펴보았으며 대부분의 개인의료정보를 생산, 보관, 관리하고 있는 의료기관 정보화에 대한 현황과 개인의료정보 유노출 실태를 살펴봄으로써 개인의료정보 보호의 필요성과 중요성을 다시 한번 부각하였다.

제1절 개념 및 특성

1. 개인정보와 개인의료정보, 개인건강정보

가. 개인정보

개인정보 보호법 제2조(정의) 제1항에 의하면 '개인정보'란 살아 있는 개인에 관한 정보로, 해당정보 하나만으로 개인을 알아볼 수 있는 경우뿐 아니라 몇 개 정보를 결합했을 때 개인을 알아볼 수 있는 정보도 개인정보라 정의하고 있다.

개인정보 보호법에 의하면 이러한 '개인정보'는 1) 살아있는 개인, 2) 특정 개인과의 관련성, 3) 특정 제한을 두지 않는 정보의 임의성, 4) 특정 개인을 구별할 수 있는 식별 가능성 등 4가지 속성에 대해 규정하고 있다. 첫째, 살아있는 개인을 규정함에 있어 법인이나 단체는 해당되지 않는 자

연인을 의미하며 다만 사망자의 정보라 하더라도 이를 통해 유족과의 관계가 나타나거나 유족의 사생활을 침해하는 경우에는 이는 유족의 정보라 판단하여 개인정보라 간주한다. 둘째, 특정 개인과의 관련성에 있어서는 한 개인에 대한 사실, 판단, 평가에 관한 정보로 성명, 주민등록번호, 생일, 주소, 바이오정보 등과 같이 정체성(identity)을 구별하거나 밝혀낼 수 있는 정보 혹은 교육상황, 재정상황, 진료 및 건강상태 등과 같이 한 개인의 과거 혹은 현재 상황이나 상태를 나타내는 정보를 의미하는 반면 직원의 평균연봉, 졸업생의 취업률 등과 같이 가공 혹은 통계화된 정보는 특정 개인과의 관련성을 찾을 수 없으므로 개인정보에 포함하지 않는다. 셋째, 정보의 임의성에 있어서는 개인정보의 종류, 형태, 성격, 처리형식 혹은 처리매체 등에 있어 특정 제한을 두지 않는 것으로 객관적인 사실에 기반한 정보에서부터 주관적 정보까지, 사실정보에서부터 부정확하고 허위정보까지, 전자화된 정보에서부터 수기정보, 영상정보, 기타 문자·숫자·음성·화상 등으로 처리된 정보까지 모두 해당된다는 점이다. 마지막으로 식별 가능성에 대해서는 성명, 주민등록번호, 학번, 사번, 고객ID, 결재정보 등과 같이 타인과 구별할 수 있는 속성 뿐 아니라 정보들을 결합하고 조합하여 특정개인을 구별할 수 있는 정보를 의미한다(행정안전부, 2011).

개인정보는 생성 및 이용영역에 따라 일반정보, 가족정보, 교육 및 훈련정보, 병역정보, 부동산정보, 소득정보, 신용정보, 의료정보, 신체정보 등 16가지 종류로 구분하기도 한다[5](표 2-1 참조). 이러한 개인정보는 시대, 기술, 인식이 변화하면서 적용대상과 범위 또한 변화하게 된다. 그 예로 정보기술 발전에 따라 '위치정보'가 수집가능해 짐에 따라 '위치정

5) 개인정보 보호 종합지원 포털 중 '안내광장',
http://www.privacy.go.kr/nns/ntc/inf/personalInfo.do, [인용 2013.10.30.].

보'가 개인정보로 간주되어 이를 보호하기 위한 '위치정보의 보호 및 이용 등에 관한 법률(일명 위치정보 보호법)'이 새롭게 제정되기도 하였다(개인정보보호위원회, 2012).

〈표 2-1〉 개인정보의 종류

구분	항 목
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술자격증 및 전문면허증, 이수한 훈련프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타 수익정보	보험 (건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과 직무태도
법적정보	전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(E-mail), 전화통화내용, 로그파일(Log file), 쿠키(Cookies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

자료: 개인정보보호 종합지원 포털사이트 중 '안내광장', http://www.privacy.go.kr/nns/ntc/inf/personalInfo.do, [인용 2013.10.30.].

개인정보는 개인, 기업, 정부차원에서 그 중요성을 지니고 있는 바, 먼저 개인차원에서는 개인정보 유출시 생명, 신체에 대한 위협, 재산상 손실, 사회적 평가저하 등과 같은 불이익을 받을 수 있으며 기업차원에서는 고객 개인정보에 대해 관리부주의로 인한 유출시 브랜드 가치 하락, 평판 악화는 물론 이로 인한 외부 협박이나 이용자의 손해배상 청구 등 직, 간접적인 재산상 손해를 감수하여야 한다. 또한 정부차원에서는 정보화사회에 대한 신뢰구축에 많은 타격을 입게 되는 등 개인이나 기업차원보다 더 많은 피해가 예상되어 보다 강한 책임을 지고 있다[6].

나. 개인의료정보와 개인건강정보

많은 이들이 의료정보, 보건의료정보, 건강정보라는 용어를 혼용하여 사용하고 있어 저자에 따라, 독자에 따라 서로 이해를 달리 할 수 있다. 그러므로 본 연구의 대상인 의료기관에서의 개인정보에 대한 이해를 같이하기 위해 본 절에서는 개인에 관한 의료정보, 개인에 관한 건강정보 즉 '개인의료정보'와 '개인건강정보'에 대해 다시한번 정리해보고자 한다.

앞에서 언급한 바와 같이 개인정보는 일반적인 정보와 구분되는 4가지 속성을 지니고 있는 바, 개인의료정보, 개인건강정보 또한 의료정보, 건강정보와 구분되는 4가지 속성을 지니고 있다 할 수 있다. 그러나 대부분 많은 이들이 이에 대해 명확한 구분없이 사용하고 있어 본 연구를 위한 문헌고찰 시 전체적인 내용 흐름상 개인의료정보, 개인건강정보의 의미를 내재하고 있다고 판단되는 경우에는 원 문에서 의료정보, 건강정보라 칭하였다 해도 이를 개인의료정보, 개인건강정보로 이해하여 분석하였다.

백윤철(2005)은 개인의료정보를 개인의 질병에 관한 진료정보가 중심

6) 개인정보 보호 포털사이트, www.i-privacy.kr, [인용 2013.06.10.].

이 되며 의료서비스에 대한 필요성을 판단하고 제공하기 위해 진료등을 통해 얻은 환자의 관련정보라 하여 환자의 기본정보에서부터 건강보험정보, 진료기록정보, 사망기록정보 등으로 분류하였다(표 2-2 참조).

〈표 2-2〉 개인의료정보의 유형

구분	내용
환자기본 정보	성명, 연령, 생년월일, 주소, 전화번호, 연락처, 근무지, 호적등본, 배우자정보 등
건강보험 및 복지 정보	건강보험정보, 장애자수첩정보 등
진료관리 정보	진료정보, 내원일자, 입원 및 퇴원일자 등
생활 정보	흡연여부, 음주여부, 정신상태 정보
의학적 정보	출생시 체중, 임신분만 관련기록, 예방접종 관련기록, 수혈여부, 가족병력 등
진료기록 정보	진단, 진료계획, 현 병력 등
지시기록 정보	처방지시 기록, 수술기록, 처치 기록 등
진료정보 교환정보	진단서 등
진료설명 및 동의 정보	설명정보, 동의정보 등
요약 정보	진료요약, 입원요약 등
사망기록 정보	사망진단서, 부검기록 등

자료: 백윤철(2005). 헌법상 환자의 의료정보에 대한 권리에 관한 연구, 헌법학 연구 제11권 제3호, pp 337~373, 한국헌법학회.

또한 장석천(2007)은 개인의료정보를 진료받는 환자를 통해 의료인이나 의료기관이 취득·보유하는 개인정보라 하면서 진찰 이전에 작성하는 환자의 기본정보, 진료단계에서 환자 증상이나 검사에 관한 정보, 그리고 이를 기초로 의사가 환자의 증상을 진단한 진단정보 등 크게 3가지로 나누기도 하였다. 박윤형(2005)과 박지용(2012)은 이를 진료정보, 혹은 개인진료정보라는 용어로 사용하고 있다.

그 외 많은 문헌들에서도 의료정보, 개인의료정보, 진료정보, 개인진료정보 등을 정의하고 있었으나 크게 다르지 않았으며 공통적으로 의료기관과 환자가 중심이 되어 의료현장에서 생성되는 모든 개인정보를 기술하고 있었다.

이와 같은 개인의료정보에 대한 특성을 살펴보면(박윤형, 2005; 한국정보보호진흥원, 2006; 장석천, 2007; 이한주, 2012) 첫째, 일신전속성이 크다는 것이다. 즉 일반적인 개인정보보다 정보주체와의 관련성이 더 크다고 할 수 있으며 이는 정보주체에 대한 식별가능성이 더 크다는 의미이기도 한다. 둘째, 정보의 이용범위가 증가하고 있다는 것이다. 개인의료정보는 환자의 진료나 치료 뿐 아니라 의학연구, 의학교육, 통계자료 작성, 고부가가치산업 창출을 위한 기반마련 등 2차적 이용이 점차 더 증가하고 있다. 셋째, 접근경로가 다양하고 이동성이 증가하고 있다는 것이다. 대부분 의료기관에서 개인의료정보가 전자적 형태로 보관됨으로써 환자진료를 위한 의료진 뿐 아니라 수납, 보험 등 행정직원, 심지어 외부 위탁운영을 수행하고 있는 전산담당자들도 접근이 가능하게 되었으며 e-Health, u-Health 보급에 따라 개인의료정보에 대한 수집·보관이 사용자 단말기에서까지 가능하게 되는 등 개인의료정보의 접근성과 이동성이 증가하고 있다. 넷째, 침해 시 일반적인 개인정보보다 그 피해가 더 크다 할 수 있다. 개인의료정보는 개인 병력 등과 같은 대부분 민감한 정보로, 타인에게 공개 시 자존감이 훼손당하고 정신적 충격을 받을 수 있으며, 근로관계에서의 불이익 또는 차별을 받을 수 있고, 사회관계에서 배제당하는 등 심각한 피해를 야기할 수 있는 것이다.

결론적으로 개인의료정보는 일반적인 개인정보보다도 정보주체와의 관련성이 크고 침해시 그 피해가 더 큰 반면, 의료정보화 및 의료패러다임 변화에 따라 접근경로와 이동성이 증가하게 됨에 따라 개인정보 보호

의 필요성과 중요성이 한층 증대되었으나, 한편 정보의 유용성 측면에서는 정보 보호 뿐 아니라 적절한 이용 및 활용과의 균형도 중요한 과제가 되고 있다.

한편, 건강정보는 앞서 언급한 의료정보를 포함하여 예방, 진단, 치료, 재활, 건강증진, 건강관리 등과 관련된 즉 건강을 유지하고 관리하는 데 필요한 포괄적인 정보로써 개인건강정보는 개인신상정보, 개인의료정보, 그리고 개인건강관리정보를 모두 포괄하여 지칭한다. 개인의료정보가 의료기관을 중심으로 수집, 이용, 관리되는 개인정보라 한다면 개인건강정보는 의료기관을 포함해 공공기관, 관련 협·단체, 건강관련 포털, 모바일 앱 등을 통해 수집되고 이용·관리되는 건강과 관련된 모든 개인정보라 할 수 있겠다.

2. 정보화 역기능, 개인정보침해와 개인정보보호

가. 정보화 역기능

정보화로 인한 순기능 뿐 아니라 정보화역기능에 대해 관심이 증가하고 있는 가운데 '정보화역기능'은 정보화 진전에 따라 컴퓨터 및 인터넷 등 정보통신수단을 이용하거나 정보통신수단에 대해 행하여지는 해킹, 바이러스 유포등 각종 컴퓨터범죄 및 기타 정보화에 수반하는 제반 문제점으로 정의하여 〈표 2-3〉과 같이 구분하기도 한다(정보통신부, 1999).

또한 사회에 경제적 피해를 끼치는 유무에 따라 정보화역기능을 적극적 정보화역기능과 소극적 정보화역기능으로 구분하기도 하고 피해파급효과가 개인에게 미치는지, 국가 또는 사회에 미치는 지에 따라 개인적 역기능과 국가/사회적 역기능으로 구분하기도 한다(한국정보보호진흥원, 2001, 표 2-4 참조).

〈표 2-3〉 정보화 역기능의 종류

구분	내용
불건전정보 유통	정보통신망을 통한 음란물, 폭력물, 반사회적 내용의 정보유통
유언비어 유포	정보통신망을 통해 사회질서를 교란하거나 지역간, 계층간 불신과 위화감을 조장하는 내용의 유언비어 유포
정보시스템 불법 침입 및 파괴	정보시스템 해킹, 컴퓨터바이러스 및 악성코드 유포, 사이버테러, 전자우편폭탄(mail bomb) 발송 등
프라이버시 침해	정보통신망에서의 개인 프라이버시 침해
개인정보 오남용	정보통신망을 통한 개인정보 유노출 및 불법 유통
인터넷을 통한 범죄행위	사이버 스토킹, 사이버도박, 인터넷사기, 인터넷을 통한 마약밀매, 매매춘·무기판매·탈세 등
암호기술의 부정사용	범죄조직 및 테러집단 증에서 범죄증거 은닉을 위한 수단으로 암호기술 사용
전자거래의 안전·신뢰성 저해	전자문서 위변조, 타인명이를 도용한 전자거래, 전자문서 작성사실 부인 등
지적재산권 침해	SW, 멀티미디어콘텐츠 불법복제, PC통신 및 인터넷상 전자문서 무단사용, 멀티미디어 편집제작물에 의한 지적재산권침해 등
전자파로 인한 피해	인체피해, 전파간섭
게임 및 인터넷 중독	게임 및 인터넷중독으로 인한 건강침해, 사회적 소외현상, 인간성 상실, 저질문화 확산 등

자료: 정보통신부(1999), 정보화역기능 방지 종합대책.

〈표 2-4〉 정보화 역기능의 유형

피해 파급대상 / 경제적 피해유무	개인적 차원의 정보화역기능	국가,사회적차원의 정보화역기능
적극적 정보화역기능	개인정보침해 전자거래피해	해킹·바이러스 피해 지적 재산권 도용
소극적 정보화역기능	스팸메일 인터넷중독	불건전 정보유통 정보격차

자료: 한국정보보호진흥원(2001), 정보화 역기능 현황과 대응방안.

나. 개인정보 침해

개인정보가 유출되면 생명, 신체에 대한 위협 뿐 아니라 재산상의 손실, 사회적 평가저하 등 다양한 불이익을 받을 수 있다. 더욱이 개인정보 유출로 인한 온라인에서의 피해는 일단 발생하면 회복이 어려울 뿐 아니라 타 게시판 및 서비스 등으로 전달됨으로써 2차 피해가 '실시간'으로 발생할 수 있다는 특성이 있으며 개인정보 유·노출의 근원을 확인하는데 많은 자원이 소요되기도 한다[7].

개인정보 침해란 정보주체의 동의없이 즉, 정당하지 않은 절차에 의해 개인정보가 수집·이용·제3자에게 제공되는 일체의 피해를 포괄하여 일컬으며(한국정보보호진흥원·개인정보분쟁조정위원회, 2007) 이러한 개인정보 침해를 일으키는 유형으로는 이용자 동의없는 개인정보 수집, 개인정보수집시 고지 또는 명시의무 불이행, 과도한 개인정보 수집, 고시·명시한 범위를 초과한 목적외 이용 또는 제3자 제공, 개인정보취급자에 의한 훼손·침해 또는 누설 등을 들 수 있다(표 2-5 참조).

이러한 개인정보 침해의 위험성은 날로 증가하고 있으며 이에 따른 신고도 폭발적으로 늘어나고 있다. 통계청의 개인정보 침해 상담 통계를 보면 2009년 3만5,167건, 2010년 5만4,832건, 2011년 12만2,215건에서 2012년 16만6,801건으로 급증하고 있다(표 2-6 참조).

---

7) 개인정보 보호 포털사이트, www.i-privacy.kr, [인용 2013.06.10.].

〈표 2-5〉 개인정보 침해유형

번호	침해유형	법률근거
1	이용자 동의없는 개인정보 수집	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조 제1항
2	개인정보수집시 고지 또는 명시의무 불이행	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조 제2항
3	과도한 개인정보 수집	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조
4	고지·명시한 범위를 초과한 목적외 이용 또는 제3자 제공	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제24조, 제24조의 제2항
5	개인정보취급자에 의한 훼손·침해 또는 누설	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조의 제2항
6	개인정보처리 위탁시 고지의무 불이행	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제25조 제1항
7	영업의 양수 등의 통지의무 불이행	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제26조 제1항
8	개인정보관리책임자 미지정	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제27조 제1항
9	개인정보보호 기술적·관리적 조치 미비	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조
10	수집 또는 제공받는 목적달성 후 개인정보 미파기	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제29조
11	동의철회·열람 또는 정정요구 등 불응	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조 제3항 및 제4항
12	개인정보 오류정정요구 접수후 미정정 정보 이용	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조 제5항
13	동의철회·열람 또는 정정을 수집방법보다 쉽게 해야할 조치 미이행	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조 제6항
14	법정대리인의 동의없는 아동의 개인정보 수집	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제31조 제1항
15	영리목적의 광고성 정보 전송	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제50조 내지 제50조의 5
16	타인정보의 훼손·침해·도용	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조
17	기타	

자료: 개인정보 보호 포털, www.i-privacy.kr, [인용 2013.06.10.].

〈표 2-6〉 개인정보 침해신고 상담건수

구분	2009	2010	2011	2012
계	35,167	54,832	122,215	166,801
개인정보 무단수집	1,075	1,267	1,623	3,507
개인정보 무단이용제공	1,171	1,202	1,499	2,196
주민번호등 타인정보도용	6,303	10,137	67,094	139,724
회원탈퇴 또는 정정요구 불응	680	826	662	717
법적용 불가 침해사례	23,893	38,414	38,172	12,915
기타	2,404	2,986	13,165	7,742

자료 : 방송통신위원회 (한국인터넷진흥원 개인정보침해신고센터 접수자료)
e-나라지표, http://www.index.go.kr/, [인용 2013.06.10.].

그 중에서도 정보주체의 개인정보에 대해 법령에 의하지 않고 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용하는 '개인정보 유출'(표준 개인정보 보호지침 제26조) 사고가 빈번하게 발생하여(표 2-7 참조) 사회문제가 되면서 개인정보 유·노출에 대한 위험성, 개인정보 보호에 대한 중요성과 필요성은 점점 부각되었고 많은 국가들이 국가적 차원에서 이를 사전 예방하고 즉각적인 조치를 취하기 위해 법제화 추진, 민간차원의 자율규제 강화 등의 노력을 기울이게 되었다.

〈표 2-7〉 국내 주요 개인정보 유출사고 현황

시기	업체	피해규모
2006~2008	하나로텔레콤	650만명
2008년 2월	옥션	1,863만명
2008년 9월	GS칼텍스	1,119만명
2010년 3월	신세계몰	330만명
2011년 4월	현대 캐피탈	175만명
2011년 7월	SK커뮤니테이션즈	3,500만명
2011년 11월	넥슨	1,320만명
2012년 4월	EBS	400만명
2012년 7월	KT	870만명

자료: 아주경제(2013.09.23.),
http://www.ajunews.com/kor/view.jsp?newsId=20130922000122#.

다. 정보보호와 개인정보 보호

‘정보보호’란 국가정보화기본법 제3조에 의하면 “정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것”이라 정의하고 있으며 ‘개인정보 보호’란 개인정보 보호 인증제 운영에 관한 규정 제2조에 의하면, 앞에서 언급한 개인정보 유출을 막기 위해 개인정보 관리체계 수립, 개인정보 처리단계별 기준·절차 준수 및 안전한 관리, 정보주체 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동이라 일컫고 있다.

이러한 ‘개인정보 보호’는 정보주체 자신의 활동이 아닌 타인에 의한 개인정보 수집·처리와 관련하여 해당 개인정보 주체의 이익을 나타내는 개념이라 할 수 있다(이인호, 2005).

한편 국가정보화기본법 제4조(국가정보화 추진의 기본원칙) 제3항에서는 국가와 지방자치단체로 하여금 국가정보화 추진과정에서 정보화의 역기능을 방지하기 위한 정보보호, 개인정보 보호 등의 대책을 마련하도록 하고 있으며 동법 제39조(개인정보 보호 시책의 마련)에서는 국가기관과 지방자치단체에서 개인정보 보호를 위한 시책을 마련토록 하고 있다.

이와 같은 정보보호는 과거에는 비밀성에 초점을 맞추어 주로 정보보안을 일컫었으며 접근통제와 같은 물리적 보호수단을 사용하였으나 네트워크화 되면서 물리적 보호수단 뿐 아니라 새로운 기술적인 방안이 필요하게 되었다.

개인정보보호의 개념에 있어 고려되어야 할 것은 프라이버시(privacy) 개념으로, 흔히들 동일한 의미로 사용되기도 한다. 프라이버시는 본래 사생활에 관한 소극적 차원에서의 방어권에서 이제는 자신의 정보를 직접 관리하고 통제하기 위한 필요를 느끼게 되면서 ‘자기정보관리통제권’이

라는 권리가 부각하게 되었다(박지용, 2012).

더욱이 개인정보의 집중화 및 맞춤형 서비스제공 등으로 인해 개인정보활동의 추적이 가능해지고, 기업의 빅브라더화 등으로 사생활침해가 더욱 더 심각해지면서 개인정보의 안전한 관리 및 활용을 위한 지속적인 제도방안을 마련할 필요가 대두되었으며(한국인터넷진흥원, 2013) 마침내 우리나라에서도 개인정보 유출 및 오·남용 등의 근절을 통해 안전하고 신뢰받는 정보사회 구현을 위해 2011년 3월 「개인정보 보호법」이 제정되어 같은해 9월부터 시행되면서 사회 각 분야에서의 개인정보보호에 대한 관심은 계속 높아지고 있다.

2012년 인터넷이용실태조사 결과에 의하면, 우리나라 '12년도 만3세 이상 인터넷이용자에 대한 이용률은 78.4%로 계속 증가하고 있는 가운데 이들 중 만12세이상 인터넷이용자의 78.8%가 인터넷으로 인해 일상생활이 편리해졌다고 생각하고 있는 반면, 64.5%는 개인정보 혹은 금융정보 등의 유출을 우려하고 있었으며 64.4%는 일탈행동 및 모방범죄가 늘어날 것을 걱정하는 등 부정적 인식도 상당히 자리하고 있는 것으로 나타났다. 이를 통해 명의도용, 개인신상정보 오남용과 같은 인터넷확산에 따른 사회문제에 대해서도 많은 우려를 나타내고 있었다(방송통신위원회·한국인터넷진흥원, 2012a).

한편, 2012년 개인대상의 정보보호실태조사 결과에 의하면, 만12-59세 인터넷이용자의 99.2%가 평소 인터넷이용 시 개인정보보호를 중요 혹은 매우중요하게 인식하고 있었으며(2011년 98.5% 대비 0.7%p 상승) 인터넷으로 인한 사회문제 중 개인정보/프라이버시 침해에 대해 94.6%가 심각 혹은 매우 심각하게 생각하고 있었다. 지난 1년간 인터넷이용자의 41.0%가 개인정보보호 관련된 조치를 취하고 있다고 응답한 반면, 공공기관 및 사업자가 실행한 개인정보보호 관련 조치정도는 그보다 낮은

29.7%, 21.0%로 인식하고 있어 상대적으로 충분히 실행하지 않는다고 판단하는 것을 미루어 짐작할 수 있다. 즉 정보보호에 대한 인식은 높아지고 있지만, 실제 조치를 취할 수 있는 지식과 이해도는 여전히 부족한 것으로 나타났다. 또한 지난 1년간 개인정보/프라이버시 침해경험률은 9.9%로 작년 대비 0.8%p 감소한 것으로 나타났으며 이러한 침해발생의 유형은 사업자관리소홀로 인한 개인정보 유출, 사업자가 동의없이 이용 혹은 제3자 제공, 사업자의 개인정보 무단수집 등이 각각 55.3%, 32.7%, 30.1% 순으로 나타났다(방송통신위원회·한국인터넷진흥원, 2012b).

2012년도 기업대상의 정보보호실태조사에서는 이용자의 개인정보를 수집하고 있는 업체 중 공식문서로 된 개인정보보호 내부관리계획이 수립되어 있는 사업체는 53.0%로 나타났으며 직원들의 개인정보보호에 대한 인식정도는 5점 만점에 4.1점, 지난 한해동안 정보보호교육을 실시한 업체는 19.8%로 사업체가 클수록 교육실시율이 높게 나타났다. 또한 개인정보를 수집하고 있는 사업체 중 35.4%는 개인정보보호를 위한 예산을 별도로 배정하고 있는 것으로 나타났다. 수집된 개인정보의 안전한 처리를 위한 기술적 조치로는 DB 접근내역에 대한 로그저장, 개인정보의 암호화저장, USB/이동형 저장장치 통제, 키보드해킹 방지 솔루션 적용, 노트북/PDA 통제 각각에 대해 49.9%, 49.9%, 47.0%, 40.5%, 36.9% 적용하고 있는 것으로 나타났다(방송통신위원회·한국인터넷진흥원, 2012c).

제2절 의료정보화와 개인의료정보보호

우리나라 의료기관에 정보화가 도입되기 시작한 시기는 의료보험이 실시된 시기와 비슷하며(전기홍외, 1994) 1990년대 접어들면서 병원정보

시스템 도입이 급격하게 증가하게 되었다.

건강보험심사평가원에서 실시한 요양기관 정보화 실태조사 결과에 따르면, 우리나라 전국 종합병원 및 병원의 정보화 현황은 처방전달시스템(OCS)의 경우, 1999년 종합병원에 대한 도입현황이 50% 못 미치던 것이 2010년에는 94%로 대부분의 종합병원에서 사용하고 있었으며 병원의 경우에도 1999년 30% 미만에서 2010년 60~70% 사용현황을 나타내고 있다. 전자의무기록시스템의 경우에도 1999년 미미한 현황에서 2010년에는 종합병원의 60%대, 병원의 50% 가까이 도입하여 사용하는 등 현저히 증가함을 나타내고 있다(건강보험심사평가원, 2005.11.29.; 경북대학교·SK c&c 컨소시엄, 2011, 표 2-8 참조).

〈표 2-8〉 우리나라 종합병원 및 병원급 의료기관의 정보시스템 도입현황

(단위: %)

구분	종합병원[주]			병원		
	1999년	2005년	2010년	1999년	2005년	2010년
외래OCS	47	89	94	23	67	70
입원OCS	44	89	94	18	58	64
외래EMR	-	9	63	10	23	48
입원EMR	-	10	64	-	21	45

주: 종합병원 결과 중 1999년 자료의 경우, 상급종합병원을 미포함한 결과이며 2005년, 2010년 자료의 경우에는 상급종합병원을 포함한 결과임.

자료: 건강보험심사평가원(2005.11.29.), 우리나라 의료정보화 수준 세계 최고 -심평원의 요양기관 종별 정보화 실태조사 결과-, 건강보험심사평가원 보도자료; 경북대학교·SK c&c 컨소시엄(2011), 요양기관 정보화 실태조사(최종보고).

2010년 실태조사 결과 중 병원정보시스템 관리방법에 있어 자체관리, 위탁관리, 자체관리와 위탁관리 병행 등 3가지 방법에 대해 알아본 결과, IT인력 부족으로 인해 종합병원에서 자체관리하는 경우는 29%, 병원에서 자체관리하는 경우는 18%의 낮은 결과를 보여주고 있다(경북대학교·

SK c&c 컨소시엄, 2011, 표 2-9 참조). 상대적으로 위탁관리 비율이 높다는 것은 자체관리에 비해 개인정보 유출 및 정보보안의 문제를 더 많이 초래할 수 있을 것으로 판단된다.

〈표 2-9〉 우리나라 의료기관의 정보시스템 관리현황

(단위: %)

구분	계	자체관리	위탁관리	자체, 위탁 관리병행
종합병원	100	29	18	52
병원	100	18	45	36

자료: 경북대학교·SK c&c 컨소시엄(2011), 요양기관 정보화 실태조사(최종보고).

이처럼 의료기관의 정보시스템 보급률이 높아지면서 대규모 디지털화가 이루어지고 의료기관의 내부 직원 뿐 아니라 외부인의 접근이 수반되며 인터넷 및 웹환경 확대, u-Health, smart-Health 등과 같은 IT기술 발전에 따라 개인의료정보에 대한 접근성과 이동성이 증가하면서 개인의료정보에 대한 침해, 유노출의 위험은 점점 더 커지고 있는 실정이다.

실제로 미국에서는 2009년 이후부터 서터메디컬재단 및 서터피지션 서비스 이용 고객의 환자 의료정보 유출을 포함해 미국 내에서 약 600여 건의 유출사건이 일어나 2,200만명의 피해자가 발생하였다고 하며[8] 우리나라에서도 의료기관 및 관련기관에서 환자개인정보에 대해 불법적인 수집, 환자의 동의없이 진료목적 이외의 사용 및 제3자제공, 의료기관의 소홀한 관리로 인한 환자정보 유출, 내부 취급자에 의한 고의적인 환자정보 유노출 사건이 지속적으로 발생되고 있다(표 2-10 참조).

8) 보안뉴스(2013.06.27.), http://www.boannews.com/media/view.asp?idx=36636&kind=1.

〈표 2-10〉 2000년 이후 언론기사화된 우리나라 의료기관에서의 개인정보 유노출 현황

번호	날짜	내용	출처
1	2002.05.22	전국 53개 병의원으로부터 해킹 및 환자관리프로그램 AS를 통한 230여만 환자 개인정보 무단 유출	아이뉴스 24
2	2003.12.04	한 유명병원 인터넷 홈페이지에 합격자명단 중 이름, 주민등록번호, 출신대학 모두 공개	YTN
3	2004.01.14	경기도 한 병원에서 환자이름과 전화번호가 적힌 미수납 오더리스트를 이면지로 잘못 활용	경향신문
4	2004.06.12	병원에서의 진료기록 관리 소홀	SBS
5	2004.07.20	경남의 한 의료원에서 수십년간 환자개인진료내역서 무단방치	뉴시스
6	2004.07.27	성형외과에서 환자 본인동의없이 홈페이지에 수술 전후 사진 무단 게재	뉴시스
7	2006.10.3	부산 모 대학병원 내부직원이 사망한 환자 주민등록번호를 유출하여 대포폰 유통	부산일보
8	2006.10.24	신용정보업체에서 20여개 병원의 환자 개인정보를 유출해 채권추심에 사용	mbc
9	2007.04.24	대전 한 대학병원 환자진료기록부 및 입원환자 명단 등 개인정보가 포함된 관련서류가 대로에 방치	대전일보
10	2007.10.11	전주 모병원 내부직원이 환자개인정보를 무단유출하여 선거인단에 불법 등록	경향신문
11	2007.10.12	익산의 한 병원 간호조무사와 컴퓨터 수리업자 등이 병원 9,800여명의 환자개인정보 무단 유출	국민일보
12	2008.08.23	대학병원 홈페이지에 개인정보 노출 심각	동아일보
13	2009.05.19	한 유명연예인에 대한 진료기록 일부 유출	노컷뉴스
14	2010.02.03	국군대구병원에서 신검정밀의뢰서를 이면지로 사용	경향신문
15	2010.03.10	경기도 모병원의 환자 개인정보 유출이 의심되는 SMS	코리아 헬스로그
16	2010.11.17	종합병원에서 정보제공에 대한 동의없이 무단 정보수집	문화일보
17	2011.04.30	국립병원이 전직 대통령의 개인의료정보 유출	서울신문
18	2011.05.04	전직 대통령의 X-선 사진 무단유출	데일리 메디
19	2011.09.29	국내 대형병원 등에서 본인 동의없이 22만 여명의 환자 개인정보를 보건의료연구원에 불법 제공(국감)	보안뉴스
20	2012.03.13	서울시장 아들의 의료정보 무단유출	뉴데일리

번호	날짜	내용	출처
21	2012.04.18	고물상에 병원처방전 폐지처분	C뉴스 041
22	2012.08.20	한 국립의료기관에서 병력지를 이면지로 사용	노컷뉴스
23	2012.09.28	600여개 산부인과에서 의료기기 판매대행 업체에 환자 개인정보 23만건 유출	조선일보
24	2012.10.22	의료기관 및 민영보험사에서 본인동의 없이 5년동안 400여건에 대해 제3자(국민연금공단) 제공	뉴스 토마토
25	2012.10.31	구글검색으로 A산부인과 홈페이지에서 회원개인정보 17여만건 무단 유출	한국일보
26	2012.11.13	경기도 도립병원들의 개인정보보호를 위한 기술적 조치 미흡	아시아 투데이
27	2013.01.25	충남 모 병원에서 입원환자 기록문서 관리 소홀	뉴스1
28	2013.07.18	개인정보 보호법 시행이후 실태점검수행 34개 의료기관 중 22개기관 위법사항 적발	데일리 메디
29	2013.08.07	S통신사 전자차트(청구소프트웨어프로그램) 설치 의료기관에서 환자동의없이 개인정보 제3자 제공	청년의사
30	2013.08.28	해킹에 의한 국내 병원들의 환자 개인정보 유출	전자뉴스
31	2013.10.02	해킹에 의한 국내 성형외과의 환자 개인정보 유출	JTBC TV

한편, 안전행정부가 개인정보 보호법 시행이후 2012년도에 실시한 총 47회 756개소에 대한 현장점검 결과, 과태료 57건, 시정조치 360건등 총 441건의 행정처분이 부과되었으며 이중 의료업의 경우에는 위반비율이 52.4%로 타 분야보다는 낮게 나타났으며(안전행정부·한국정보화진흥원, 2013.09.06., 표 2-11 참조), 의료·보건분야에서의 주요 위반내용으로는 동의시 필수고지사항 누락, 고유식별정보 별도동의 위반, 개인정보 보호책임자 미지정, 접근권한관리의무 위반 등으로 나타났다(보안뉴스, 2013.07.31., 표 2-12 참조).

〈표 2-11〉 주요업종별 위반비율 현황

구분	계	공공기관	민간분야					
			금융	운송업	의료업	학원	협회/연맹	기타
점검기관(개소)	441	74	37	27	21	25	25	232
위반기관(개소)	364	49	33	17	11	20	17	217
위반비율(%)	82.5	66.2	89.2	63.0	52.4	80.0	68.0	93.5

자료: 안전행정부·한국정보화진흥원(2013.09.06.), 개인정보 위반사례와 현장 점검결과.

〈표 2-12〉 주요업종별 위반내용

업종구분		위반내용
공공기관		- 개인정보파일 미등록, 보유기간 과다산정 및 미파기등 - 로그인/실명확인시 전송구간 암호화 미조치
민간분야	금융	- 선택사항 미동의시 서비스제공 의무 위반 - 수탁회사 관리감독 소홀 - PC저장시 암호화 미조치, 보험서류관리 소홀등 - 개인영상정보(비밀번호, 계좌번호)과도한 수집 - 개인영상정보 파기조치 미실시, 열람기록 관리위반 등
	유통·운송	- 개인정보 최소수집원칙 위반, 고유식별정보 별도동의 위반 - 위탁처리시 별도조치사항 누락, 접속기록 관리 위반등 - CCTV 안내판 설치누락, 관리방침 수립·공개 미이행 - 열람·제공시 기록관리 의무 위반등
	의료·보건	- 동의시 필수고지사항 누락, 고유식별정보 별도동의 위반 - 개인정보보호책임자 미지정, 접근권한관리 의무 위반
	학원·호텔	- 동의시 필수고지사항 누락, 고유식별정보 별도동의 위반 - 개인정보 처리정치 미조치, 전송구간 암호화 미조치 등
	협회·단체	- 동의시 필수고지사항 누락, 수집·제공 구분동의 위반 - 전송구간 암호화 미조치, 비밀번호 작성규칙 미수립·미적용
	기타	- 동의시 필수고지사항 누락, 고유식별정보 별도동의 위반 - 개인정보처리방침 미수립, 전송구간 암호화 미보치 등

자료: 보안뉴스(2013.07.31.), 개인정보보호 현장점검 사례와 향후 추진방향,
http://www.boannews.com/media/view.asp?idx=37114&kind=1.

그러나 한편으로 우리나라 소위 '빅5'라고 하는 대형 의료기관 조차도 보안 및 보호 전담인력이 거의 없는 상황이고, 다양한 정보기술이 도입되고는 있으나 환자 개인정보보호를 위한 많은 노력(솔루션구축, 인력충원 등)과 관리수준이 타 산업에 비해 미흡한 것은 정부가 의료계에 대해 타 산업에 비해 규제를 덜 하기 때문이라는[9] 해석이 있기도 하다.

9) 디지털타임스(2013.01.17.),
http://www.dt.co.kr/contents.html?article_no=2013011702011060785002.

제3장 의료부문 개인정보보호관련 정책현황

제1절 관련 법·제도

제2절 관련 현황조사

제3절 관련 인증제도

3 의료부문 개인정보보호관련 정책현황

제3장에서는 개인의료정보 보호를 위한 정부차원의 노력과 이에 대한 최근 추세를 파악하기 위해 우리나라의 개인정보 보호법, OECD, EU, 미국의 관련 가이드라인 및 지침, 우리나라의 관련 지침 등을 살펴보았으며 개인정보 보호 (관리)현황, 문제점 및 대책을 마련하기 위해 주기적으로 수행하고 있는 기존의 각종 조사내용 및 조사결과에 대해 알아보았다. 또한 민간자율적인 노력으로써 관련 인증제도에 대한 내용과 현황에 대해서도 알아보았다. 본 장은 특히 제4장에서 다룰 본 연구에서의 조사설계 시 조사항목 수립, 그리고 제5장의 정책대안 모색에 대한 근거를 마련함에 그 의의를 두고 있다.

제1절 관련 법·제도

법령의 입법방식에는 하나의 법률로 공공 및 민간부문을 포괄적으로 규제하는 통합(omnibus)방식, 공공과 민간을 각각 별개 법률로 규제하는 분할(segment)방식, 그리고 개별영역별 해당 법률로 규제하는 개별방식 등 3가지로 나눌 수 있다(백윤철, 2008).

우리나라는 1980년대부터 정부차원의 본격적인 정보화가 추진되면서 이에 따른 역기능의 우려도 부각되었으며 그 중 정보보호에 대한 중요성으로 인해 관련제도가 마련된 것은 1995년 제정된 정보화촉진기본법이 그 시초라 할 수 있다(한국인터넷진흥원, 2013). 이후 공공과 민간이 별개의 법률로 규제하는 분할방식으로 시행되어 오다 2011년 3월 일반법

인 개인정보 보호법이 제정되어 같은해 9월 30일에 본격적으로 시행되는 즉 통합방식으로 개인정보 보호 원칙이 정립되었다. 그 후 현재 개인정보 보호와 관련한 국내 주요 법제도에는 일반법으로 개인정보 보호법이 있고, 개별법으로 민간부문에서는 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등이 있다.

본 절에서는 개인정보 보호 및 개인의료정보 보호에 대한 법·제도를 살펴보기 위해 우리나라 개인정보 보호법을 중심으로 하여 OECD 프라이버시 가이드라인, EU의 개인정보 보호 지침, 미국 HIPAA 의 프라이버시 규칙 등을 살펴보고 아울러 행정안전부 고시인 개인정보의 안전성 확보 조치 기준과 표준 개인정보 보호 지침, 그리고 보건복지부 개인정보 보호 기본 지침에 대해 간단히 살펴보고자 한다. 이를 통해 국내외 개인정보 보호, 개인의료정보 보호에 대한 추세를 파악하고자 하였다.

1. 개인정보 보호법

개인정보 보호법은 “개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위해 개인정보 처리에 관한 사항을 규정함”을 목적으로 한 일반법으로 2011년 3월 29일 법률 제10465호로 제정되어 동년 9월 30일부터 시행되었다.

개인정보 보호법은 적용대상주체에 있어 개인정보를 처리하는 공공기관에서 민간처리자까지 확대하고, 대상정보도 기존 전자정보 뿐 아니라 수기문서 등 모든 형태의 정보를 포괄함으로써 종래 존재하였던 정보 보호의 사각지대를 해소하였다는 점에서 큰 의미를 가지며 개인정보 보호에 관한 일반원칙을 제시하고 개인정보의 수집, 활용 및 파기라는 단계적 처리절차를 규율하고 있다는 점도 동 법의 중요한 성과라 할 수 있다(박

지용, 2012).

동 법은 총칙, 개인정보 보호정책의 수립등, 개인정보의 처리, 개인정보의 안전한 관리, 정보주체의 권리 보장, 개인정보 분쟁조정위원회, 개인정보 단체소송, 보칙, 벌칙 등 총 9개 장 75개 조, 그리고 부칙으로 구성되어 있다(표 3-1 참조).

〈표 3-1〉 개인정보 보호법 구성내용

장 구성		조 구성
제1장 총칙		제1조(목적) 제2조(정의) 제3조(개인정보 보호 원칙) 제4조(정보주체의 권리) 제5조(국가 등의 책무) 제6조(다른 법률과의 관계)
제2장 개인정보 보호정책의 수립 등		제7조(개인정보 보호위원회) 제8조(보호위원회의 기능 등) 제9조(기본계획) 제10조(시행계획) 제11조(자료제출 요구 등) 제12조(개인정보 보호지침) 제13조(자율규제의 촉진 및 지원) 제14조(국제협력)
제3장 개인 정보의 처리	제1절 개인정보의 수집, 이용, 제공 등	제15조(개인정보의 수집·이용) 제16조(개인정보의 수집 제한) 제17조(개인정보의 제공) 제18조(개인정보의 이용·제공 제한) 제19조(개인정보를 제공받은 자의 이용··제공 제한) 제20조(정보주체 이외로부터 수집한 개인정보의수집 출처 등 고지) 제21조(개인정보의 파기) 제22조(동의를 받는 방법)
	제2절 개인정보의 처리 제한	제23조(민감정보의 처리 제한) 제24조(고유식별정보의 처리 제한) 제25조(영상정보처리기기의 설치·운영 제한) 제26조(업무위탁에 따른 개인정보의 처리 제한) 제27조(영업양도 등에 따른 개인정보의 이전 제한) 제28조(개인정보취급자에 대한 감독)
제4장 개인정보의 안전한 관리		제29조(안전조치의무) 제30조(개인정보 처리방침의 수립 및 공개) 제31조(개인정보 보호책임자의 지정)

장 구성	조 구성
	제32조(개인정보파일의 등록 및 공개) 제33조(개인정보 영향평가) 제34조(개인정보 유출 통지 등)
제5장 정보주체의 권리 보장	제35조(개인정보의 열람) 제36조(개인정보의 정정·삭제) 제37조(개인정보의 처리정지 등) 제38조(권리행사의 방법 및 절차) 제39조(손해배상책임)
제6장 개인정보 분쟁조정위원회	제40조(설치 및 구성) 제41조(위원의 신분보장) 제42조(위원의 제척·기피·회피) 제43조(조정의 신청 등) 제44조(처리기간) 제45조(자료의 요청 등) 제46조(조정 전 합의 권고) 제47조(분쟁의 조정) 제48조(조정의 거부 및 중지) 제49조(집단분쟁조정) 제50조(조정절차 등)
제7장 개인정보 단체소송	제51조(단체소송의 대상 등) 제52조(전속관할) 제53조(소송대리인의 선임) 제54조(소송허가신청) 제55조(소송허가요건 등) 제56조(확정판결의 효력) 제57조(민사소송법의 적용 등)
제8장 보칙	제58조(적용의 일부 제외) 제59조(금지행위) 제60조(비밀유지 등) 제61조(의견제시 및 개선권고) 제62조(침해 사실의 신고 등) 제63조(자료제출 요구 및 검사) 제64조(시정조치 등) 제65조(고발 및 징계권고) 제66조(결과의 공표) 제67조(연차보고) 제68조(권한의 위임·위탁) 제69조(벌칙 적용 시의 공무원 의제)
제9장 벌칙	제70조 ~ 제73조(벌칙) 제74조(양벌규정) 제75조(과태료)
부칙	시행일,다른법률의 개정 등

자료: 국가법령정보센터 사이트, http://www.law.go.kr/, [인용 2013.06.15.].

동 법 제3조에서는 개인정보 보호 원칙을 제시하고 있는 바, 「OECD 프라이버시 8 원칙」, 「EU 개인정보보호지침」, 「APEC 프라이버시 원칙」 등을 고려하여 기술하고 있다(행정안전부, 2011.12., 표 3-2 참조).

〈표 3-2〉 개인정보 보호법의 개인정보 보호원칙

개인정보 보호법의 개인정보 보호원칙
- 목적에 필요한 최소정보의 수집(제1항) - 사생활 침해를 최소화하는 방법으로 처리(제6항) - 익명처리의 원칙(제7항)
- 처리목적 내에서 정확성, 완전성, 최신성 보장(제3항)
- 처리목적의 명확화(제1항)
- 목적 범위내에서 적법하게 처리, 목적의 활용금지(제2항)
- 권리침해 가능성 등을 고려하여 안전하게 관리(제4항)
- 개인정보 처리방침 등 공개(제5항)
- 열람청구권 등 정보주체의 권리보장(제5항)
- 개인정보처리자의 책임준수, 신뢰확보 노력(제8항)

자료: 행정안전부(2011.12.), 개인정보 보호법령 및 지침·고시 해설.

이러한 개인정보 보호법은 개인정보처리자가 〈표 3-3〉과 같이 개인정보 처리단계(생명주기, life cycle)에 따른 침해를 예방하기 위한 개인정보 보호 조치를 이행하도록 제도화하고 있다.

이러한 개인정보 보호법은 시행 2년만에 정부·공공기관 및 민간기업의 주민번호 수집을 금지하고 주민번호에 대한 관리책임성을 강화하는 등의 내용을 주요골자로 하여 2013년 8월 6일 개정되었으며 2014년 8월부터 시행예정이다(표 3-4 참조). 이로 인해 인터넷기업을 물론이고 일반 기업들에게도 보다 강화된 개인정보 보호대책이 요구되며 특히 주민번호 수집·이용에 많은 제재를 가하게 되었다.

〈표 3-3〉 개인정보 처리단계별 주요 침해내용

수집단계	저장 및 관리단계	이용 및 제공단계	파기단계
동의 또는 법적근거 없이 개인정보 수집	조직 내부취급자에 의한 개인정보 유출, 훼손 변경등	동의 또는 법적 근거없이 개인정보 무단 제공/공유	수집 및 목적달성후 개인정보 미파기
동의 또는 법적 근거없이 정보주체로부터 수집	외부인의 불법적 접근에 의한 개인정보 유출 및 훼손변경	당초 수집목적을 넘어서는 개인정보 이용	개인정보 삭제요구 불응
법정대리인의 동의 없는 개인정보 수집	사업자의 인식부족, 과실 등으로 인한 개인정보 공개	타인의 개인정보 무단 이용	
서비스 이용과 관련 없는 과도한 개인정보 수집	기술적 관리적 조치 미비로 인한 개인정보 유출		
해킹 등 불법수단에 의한 개인정보 수집 등	고객의 개인정보 클레임에 대한 불응 또는 미조치 등		

자료: 개인정보보호위원회(2012), 2012 개인정보보호 연차보고서.

〈표 3-4〉 2014년 8월부터 시행예정인 개인정보 보호법 개정으로 달라지는 내용

구분	현 행	개정안
주민번호 수집·이용	- ①정보주체의 별도 동의, ②법령에 구체적인 근거가 있는 경우 수집·이용	- ①법령에 구체적인 근거가 있는 경우 ②정보주체나 제3자의 급박한 생명·신체·재산상 이익을 위해 명백히 필요한 경우 ③안전행정부령으로 정하는 경우만 수집·이용 ※ 정보주체의 동의에 의한 수집 금지 → 위반시 3천만원 이하 과태료 - 旣 수집 주민번호는 법령에 구체적인 근거가 없는 경우 법 시행 후 2년 이내 파기
과징금 제도	- 없음	- 주민번호 유출시 5억원 이하의 과징금 부과 - 단, 안전성 확보조치를 모두 이행한 경우는 제외
CEO 징계권고	- 개인정보 법규 위반시 책임있는 자를 징계할 것을 그 소속 기관·단체 등의 장에게 권고	- 책임있는 자에 해당 기관 대표자 및 책임있는 임원이 포함된다는 것을 명확화

자료: 안전행정부(2013.7.30.), 공공기관도 주민번호 수집 엄격히 제한, 안전행정부 보도자료.

2. OECD 프라이버시 가이드라인

OECD는 1980년 '프라이버시 및 국가간 개인정보 이전에 대한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 이하 프라이버시 가이드라인)'을 제정하였는바, 이는 개인정보 수집 및 관리에 관한 내용을 중심으로 하여 세계 각국의 개인정보 관련법률과 지침개발을 위한 기초자료로 활용되어 오고 있다(윤재석, 2012.12.12.). 이는 개인정보 보호와 관련하여 국제조직 차원에서 관심을 가지고 추진한 최초의 노력이라 할 수 있다.

OECD 프라이버시 가이드라인은 수집제한의 원칙, 정보내용 정확성의 원칙, 목적 명확성의 원칙, 이용제한의 원칙, 안전성 확보의 원칙, 공개의 원칙, 정보주체 참여의 원칙, 책임의 원칙 등 모두 8개 원칙으로 구성되어 있으며 1980년 처음 제정된 이후 2008년 개정되었고, 최근 2013년 7월 11일 OECD 이사회에서 다시 한번 개정안을 채택하였다.

2013년 7월 개정된 8원칙은 〈표 3-5〉와 같으며 해당 가이드라인에는 첫째, 위험관리에 기초한 접근법에 의해 개인정보 보호의 현실적 이행에 초점을 두었으며 둘째, 향상된 상호운용성에 기초하여 글로벌 차원의 개인정보 보호를 짚어보는 노력이 필요하다는 2가지 주제를 포함하고 있다(한국정보화진흥원, 2013.10.).

3. EU 개인정보 보호지침

EU는 1995년 10월 EU 회원국 시민들의 기본권과 자유, 특히 개인정보 처리와 관련된 개인의 프라이버시를 보호하기 위해 '개인정보 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 95/46/EC 지침(이하

개인정보 보호지침)'을 채택하였다(김기열, 2010). 이러한 지침(directive)은 회원국들을 대상으로 적용되는 EU 차원의 최초 입법형식으로 정보처리자의 의무, 정보주체의 권리, 제3국으로의 정보이전 금지, 독립기구 설치 등을 주요 내용으로 구성하고 있다(전은정외, 2012, 표 3-6 참조).

〈표 3-5〉 OECD 프라이버시 가이드라인의 8원칙(2013년 개정)

구분	내용
1. 수집제한의 원칙 (Collection Limitation principle)	- 개인정보 수집에는 제한이 있어야 하고, 정보는 적법하고 공정한 방법에 의해 얻어져야 하며, 정보주체의 인지 또는 동의가 있는 적절할 경우에 수집하여야 함.
2. 정보내용 정확성의 원칙 (Data Quality principle)	- 개인정보는 사용목적과 관계가 있어야 하고 그 목적에 필요한 한도 내에서 정확하고, 완전하며, 최신의 것이어야 함.
3. 목적 명확성의 원칙 (Purpose Specification principle)	- 개인정보 수집목적은 수집 이전 및 당시에 명시되어야 하며, 개인정보 이용은 명시된 수집목적 또는 수집시 목적, 목적 변경시 명시되는 목적과 상충하지 않아야 함.
4. 이용제한의 원칙 (Use Limitation principle)	- 개인정보는 명시된 이외의 목적으로 공개되거나 이용가능 또는 기타 사용될 수 없음. 단, 정보주체의 동의가 있는 경우 법률에 의해 허가된 경우에는 가능함.
5. 안전성 확보의 원칙 (Security Safeguards principle)	- 개인정보는 손실 또는 권한없는 접근, 파괴, 사용, 수정 또는 공개에 대한 적절한 안전조치에 의해 보호되어야 함.
6. 공개의 원칙 (Openness principle)	- 개인정보와 관련하여 개발, 실행, 정책에 대한 전반적인 공개방침이 있어야 하고, 그 방법은 정보관리자의 신원 및 주소를 비롯하여 개인정보의 존재와 성질, 정보의 이용목적을 용이하게 확인할 수 있는 것이어야 함.
7. 정보주체 참여의 원칙 (Individual Participation principle)	- 개인(정보주체)은 정보관리자로부터 또는 기타 방법으로 정보관리자가 자신들에 대한 정보를 보유하고 있는지에 대해 확인할 권리를 가짐. - 자신에 관한 정보와 통신할 수 있는 권리를 가짐. - 위의 2가지 요청이 거부된 경우, 그 사유를 알고 이의를 제기할 수 있는 권리를 가짐. - 자신의 정보와 관련된 정보에 이의를 제기하고 이의제기가 수락된 경우, 그 정보를 삭제, 정정, 완성, 수정할 수 있는 권리를 가짐.
8. 책임의 원칙 (Accountability principle)	- 정보관리자는 상기 원칙들을 실행하기 위한 조치를 따라야 하는 책임이 있음.

자료: 한국정보화진흥원(2013.10.), OECD 2013년 개정 개인정보보호 가이드라인, 개인정보보호 주간동향 제30호.

〈표 3-6〉 EU 개인정보 보호지침의 주요내용

구분	내용
적용범위	- 물적범위: 자동 처리되는 개인정보 및 구조화된 파일링시스템에 포함되는 개인정보 - 인적범위: 자연인의 개인정보
적용제외 영역	- 국가안보, 공공의 안전 및 방위를 위한 개인정보 처리 - 형사법 영역에서의 개인정보 처리 - 서신왕래와 같은 지극히 개인적이고 사적인 목적의 개인정보 처리 - 언론보도, 문학,예술적 표현을 위한 개인정보 처리
정보처리자의 의무	- 공정하고 적법한 개인정보 처리 - 정보처리 목적 명시 - 정보처리 목적과의 적절성, 관련성, 비례성 유지 - 개인정보 정확성과 최신성 확보 - 기술적, 조직적 보안조치 확보 - 감독기구에 정보처리에 대하여 고지
정보주체의 권리	- 정보처리의 전반적인 사항에 대하여 통지받을 권리 - 정보처리에 대해 협의할 권리 - 자신의 개인정보에 대해 수정을 요구할 권리 - 특정 상황에서의 개인정보 처리에 대해 반대할 권리
제3국으로의 정보이전 금지	- 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보 이전 금지
독립기구의 설치	- 회원국 내 독립적인 개인정보 보호기구 설치

자료: 전은정외(2012), 유럽의 개인정보보호 법·제도 동향, 정보보호학회지 제22권 제2호, pp58~72.

이러한 EU의 개인정보 보호지침은 한층 강화되어 새로운 개인정보 보호 규칙이 2012년 1월 25일 공표되었는 바, 새로 공표된 안은 다섯가지 특징을 지니고 있다. 첫째, 지침(directive)이 아닌 규칙(regulation)의 형식을 취하고 있으며 둘째, 새로운 정보기본권으로서 '잊혀질 권리'를 도입하고 있다. 셋째, 개인정보 감독기관인 단일의 '유럽정보보호위원회(European Data Protection Board)' 설치를 포함하고 있으며 넷째, 위반 시 보다 강력한 제재규정을 두고 있고 마지막으로 다섯째, 11장 91조로 이루어진 상당히 방대한 체계를 띠고 있는 등 그 내용과 효력을 한층 강화한 것으로 나타났다(함인선, 2012). 그러나 2013년 10월 유럽 정

상회담에서 개정시한 연기 혹은 개정추진 반대의견이 대두되어 개정이 불투명한 상태에 있다(아시아투데이, 2013.10.26.).

4. 미국의 HIPAA(Health Insurance Portablility and Accountability Act) 프라이버시 규칙

미국은 다른 국가와 달리 개인정보 보호를 위해 프라이버시법과 더불어 공공, 금융, 통신, 의료, 통신 등 영역별 별도의 개별 법률을 마련하고 있다(김기열, 2010). 그 중에서 의료와 관련해서 개인정보 보호를 위해서는 1996년 연방의회에서 제정된 '의료보험의 이전과 그에 수반하는 책임에 관한 법률[10]'(Health Insurance Portability and Accountability Act, 이하 HIPAA)인 개별법에서 다루어지고 있다.

HIPAA는 미국 전역에서 주를 초월하여 의료보험에 대한 이전이 이루어질 수 있게 하기 위해 제정된 법으로 의료정보의 표준화, 안전보호, 프라이버시 보호 등과 관련된 규정을 담고 있다. 이는 5개 주제(Title)로 구성되어 있으며 그 중 프라이버시 및 보안규정은 제2편(Title Ⅱ)에서 다루고 있고(HIPAA 프라이버시 규칙이라 불리움) 2003년 4월 14일 공표되어 2004년 4월 14일까지 규정준수가 의무화되었다(백윤철, 2005).

이러한 HIPAA 프라이버시 규칙은 전자적 형태 혹은 종이기반 형태 모두 적용되며 이에 포함된 환자의 권리는 프라이버시 관행에 대한 통지권, 열람접근권, 정정청구권, 공개내역 수급권, 제한요청권, 비밀 의사소통요청권 등이 있다(김동수·김민수, 2006, 표 3-7 참조).

최근 미국 정부는 의료서비스 제공자와 건강 보험 민원을 처리하는 기관간의 책임을 명확히 하고, 사고 발생시 보건부(HHS)로 보고토록 하는

10) '건강보험책임법'이라 불리우기도 함.

새로운 규정을 개정하였다(데일리시큐, 2013.01.23.).

〈표 3-7〉 미국 HIPAA 프라이버시 규칙에 포함된 환자의 권리

구분	내용
프라이버시 관행에 대한 통지권	법 적용기관은 특별한 예외경우를 제외하고 반드시 프라이버시 관행(practice)을 알려주어야 함.
열람접근권	정보주체는 특별한 예외경우를 제외하고 자신의 지정된 의료정보에 대한 검토 및 사본 획득권리를 가짐(정신과 상담노트, 법률소송을 위한 준비한 정보 등은 예외로 함).
정정청구권	정보주체는 자신의 의료정보가 부정확하거나 완전하지 않은 경우, 이를 수정할 권리를 가짐.
공개내역수급권	정보주체는 최대 6년간의 자신의 개인의료정보 공개내역을 알아볼 권리가 있음.
제한요청권	정보주체는 자신의 개인의료정보 사용제한을 요청할 권리가 있음.
비밀 의사소통 요청권	정보주체는 지정된 주소 혹은 전화번호를 통해 자신의 개인의료정보 제공 요청 등과 같이 비밀 의사소통 요청권리가 있음.

자료: 김동수·김민수(2006), e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향, 정보화정책 제13권 제4호, pp128~148, 서울: 한국정보화진흥원.

5. 개인정보의 안전성 확보조치 기준

'개인정보의 안전성 확보조치 기준(행정안전부고시 제2011-43호, 2011.9.30., 제정)'은 개인정보 보호법 제24조(고유식별정보의 처리 제한) 제3항 및 제29조(안전조치의무), 개인정보 보호법 시행령 제21조(고유식별정보의 안전성 확보 조치), 제30조(개인정보의 안전성 확보 조치)에 따라 개인정보처리자가 개인정보를 처리함에 있어 개인정보가 분실·도난·유출·변조·훼손되지 않도록 안전성을 확보하기 위한 세부적인 기준을 정하고 있다.

이와 같은 '개인정보의 안전성 확보조치 기준'은 목적, 정의, 내부관리계획의 수립·시행, 접근 권한의 관리, 비밀번호 관리, 접근통제 시스템 설

치 및 운영, 개인정보의 암호화, 접속기록의 보관 및 위·변조 방지, 보안프로그램 설치 및 운영, 물리적 접근방지 등 10개의 조와 부칙으로 구성되어 있다(국가법령정보센터 사이트, 표 3-8 참조).

〈표 3-8〉 '개인정보의 안전성 확보조치 기준' 구성내용

장 구성	조 구성
제1조	목적
제2조	정의
제3조	내부관리계획의 수립·시행
제4조	접근 권한의 관리
제5조	비밀번호 관리
제6조	접근통제 시스템 설치 및 운영
제7조	개인정보의 암호화
제8조	접속기록의 보관 및 위·변조 방지
제9조	보안프로그램 설치 및 운영
제10조	물리적 접근 방지
부칙	시행일, 영상정보처리기기에 대한 안전성 확보조치의 적용 제외, 전산센터.클라우드컴퓨팅센터 등의 운영환경에서의 안전조치

자료: 국가법령정보센터 사이트, http://www.law.go.kr/, [인용 2013.06.15.].

6. 표준 개인정보 보호지침

'표준 개인정보 보호지침(행정안전부고시 제2011-45호, 2011.9.30., 제정)'은 개인정보 보호법 제12조(개인정보 보호지침) 제1항에 따라 개인정보처리자가 준수하여야 하는 개인정보의 처리에 관한 기준, 개인정보 침해 유형 및 예방조치 등에 관한 세부적인 사항을 규정하고 있다.

이러한 '표준 개인정보 보호지침'은 총칙, 개인정보 처리 기준, 영상정보처리기기 설치·운영, 공공기관 개인정보파일 등록·공개, 보칙 등 5개 장으로 구성되어 있으며 이는 총 67개 조로 구성되어 있다(국가법령정보센터 사이트, 표 3-9 참조).

〈표 3-9〉 '표준 개인정보 보호지침' 구성내용

장 구성	조 구성
제1장 총칙	제1조(목적) 제2조(용어의 정의) 제3조(적용범위) 제4조(개인정보 보호 원칙) 제5조(다른 지침과의 관계)
제2장 개인정보 처리기준	제6조(개인정보의 수집) 제7조(정보주체의 사전 동의를 받을 수 없는 경우) 제8조(개인정보의 제공) 제9조(개인정보의 목적 외 이용 등) 제10조(개인정보 수집 출처 등 고지) 제11조(개인정보의 파기방법 및 절차) 제12조(법령에 따른 개인정보의 보존) 제13조(동의를 받는 방법) 제14조(법정대리인의 동의) 제15조(민감정보 처리) 제16조(고유식별정보 처리에 대한 동의) 제17조(주민등록번호 이외의 회원가입 방법 제공) 제18조(개인정보취급자에 대한 감독) 제19조(수탁자의 선정 시 고려사항) 제20조(개인정보 보호 조치의무) 제21조(정보주체와 재위탁의 관계) 제22조(개인정보 보호책임자의 지정 등) 제23조(개인정보 보호책임자의 공개) 제24조(개인정보 보호책임자의 교육) 제25조(교육계획의 수립 및 시행) 제26조(개인정보의 유출) 제27조(통지시기 및 항목) 제28조(통지방법) 제29조(개인정보 유출신고) 제30조(개인정보 열람 연기 사유의 소멸) 제31조(개인정보이 정정·삭제) 제32조(개인정보의 처리정지) 제33조(권리행사의 방법 및 절차) 제34조(개인정보 처리방침의 공개) 제35조(개인정보 처리방침의 변경) 제36조(개인정보 처리방침의 작성기준 등) 제37조(필수적 기재사항) 제38조(임의적 기재사항)
제3장 영상정보처리기기 설치·운영	제39조(적용범위) 제40조(영상정보처리기기 운영·관리 방침) 제41조(관리책임자의 지정)

장 구성	조 구성
	제42조(사전의견 수렴) 제43조(안내판의 설치) 제44조(개인영상정보 이용·제3자 제공등 제한 등) 제45조(보관 및 파기) 제46조(이용·제3자 제공·파기의 기록 및 관리) 제47조(영상정보처리기기 설치 및 관리 등의 위탁) 제48조(정보주체의 열람등 요구) 제49조(개인영상정보 관리대장) 제50조(정보주체 이외의 자의 개인영상정보 보호) 제51조(개인영상정보의 안전성 확보를 위한 조치) 제52조(개인영상정보처리기기의 설치·운영에 대한 점검)
제4장 공공기관 개인정보파일 등록·공개	제53조(적용대상) 제54조(적용제외) 제55조(개인정보파일 등록 주체) 제56조(개인정보파일 등록 및 변경 신청) 제57조(개인정보파일 등록 및 변경 확인) 제58조(개인정보파일 표준목록 등록과 관리) 제59조(개인정보파일의 파기) 제60조(개인정보파일 등록 사실의 삭제) 제61조(등록·파기에 대한 개선권고) 제62조(개인정보파일대장 작성) 제63조(개인정보파일 이용·제공 관리) 제64조(개인정보파일 보유기간의 산정) 제65조(개인정보파일 현황 공개 및 방법)
제5장 보칙	제66조(친목단체에 대한 벌칙조항의 적용배제) 제67조(처리 중인 개인정보에 관한 경과조치)

자료: 국가법령정보센터 사이트, http://www.law.go.kr/, [인용 2013.06.15.].

7. 보건복지부 개인정보보호 기본지침

‘보건복지부 개인정보보호 기본지침’은 복지부와 그 소속기관 및 산하 공공기관이 보유하고, 관리하고 있는 개인정보에 대해 처리하는 기준과 개인정보 침해 유형 및 예방조치 등에 관한 세부적인 내용을 규정하고 있으며 총칙, 개인정보 보호체계, 개인정보 처리단계별 준수사항, 개인정보의 안전성 확보조치, 개인정보 영향평가 및 유출대응, 영상정보처리기기 설치·운영, 개인정보 보호 실태점검 및 통합관제센터 운영, 부칙 등 8개

장으로 구성되어 있다(보건복지부, 2012.01., 표 3-10 참조). 한편, 2013년 11월 현재 보건복지부 개인정보보호 기본지침은 개정 중으로 2014년도에는 개정된 기본지침이 배포될 예정으로 있다.

〈표 3-10〉 '보건복지부 개인정보보호 기본지침' 구성내용

장 구성		조 구성
제1장 총칙		제1조(목적) 제2조(용어의 정의) 제3조(적용범위) 제4조(개인정보 보호 원칙) 제5조(다른 지침과의 관계)
제2장 개인정보 보호체계	제1절 개인정보보호 책임자	제6조(개인정보 보호업무 부서의 지정 등) 제7조(개인정보 보호책임자의 지정 및 임무) 제8조(개인정보 보호책임자의 공개) 제9조(개인정보 분야별 책임관의 지정 및 임무)
	제2절 개인정보보호 협의회	제10조(개인정보보호협의회 구성) 제11조(개인정보보호협의회 운영) 제12조(개인정보보호협의회 기능)
	제3절 보건복지부 개인정보 기본계획	제13조(보건복지부 개인정보보호 기본계획 수립) 제14조(보건복지부 개인정보보호 시행계획) 제15조(개인정보보호 교육)
제3장 개인정보 처리 단계별 준수사항	제1절 개인정보 수집 및 보유	제16조(개인정보의 수집) 제17조(개인정보 수집 출처 등 고지) 제18조(정보주체의 사전 동의를 받을 수 없는 경우) 제19조(동의를 받는 방법) 제20조(법정대리인의 동의) 제21조(민감정보 처리에 대한 동의) 제22조(고유식별정보 처리에 대한 동의) 제23조(주민등록번호 이외의 회원가입 방법 제공)
	제2절 개인정보 파일 등록	제24조(적용제외) 제25조(개인정보파일 등록 주체) 제26조(개인정보파일 등록 및 변경 신청) 제27조(개인정보파일 등록 및 변경 확인) 제28조(개인정보파일 표준목록 등록과 관리)
	제3절 개인정보 제공 및 파기	제29조(개인정보의 제공) 제30조(개인정보의 이용·제공 제한) 제31조(개인정보의 목적 외 이용 등) 제32조(개인정보를 제공받은 자의 이용·제공 제한)

장 구성		조 구성
		제33조(민감정보의 처리 제한) 제34조(고유식별정보의 처리 제한) 제35조(개인정보의 파기방법 및 절차) 제36조(법령에 따른 개인정보의 보존) 제37조(개인정보파일의 파기) 제38조(개인정보파일 등록 사실의 삭제) 제39조(등록·파기에 대한 개선권고)
	제4절 개인정보파일의 관리 및공개	제40조(개인정보파일대장 작성) 제41조(개인정보파일 이용·제공 관리) 제42조(개인정보파일 보유기간의 산정) 제43조(개인정보파일 현황 관리)
	제5절 개인정보처리의 위탁	제44조(업무위탁에 따른 개인정보의 처리 제한) 제45조(수탁자 선정 시 고려사항) 제46조(개인정보 보호 의무) 제47조(정보주체와 재위탁의 관계)
	제6절 개인정보 주체의 권리보장	제48조(개인정보 열람 연기 사유의 소멸) 제49조(개인정보의 정정·삭제) 제50조(개인정보의 처리정지) 제51조(권리행사의 방법 및 절차)
	제7절 개인정보 처리방침	제52조(개인정보 처리방침의 공개) 제53조(개인정보 처리방침의 변경) 제54조(개인정보 처리방침의 작성기준 등) 제55조(필수적 기재사항) 제56조(임의적 기재사항)
제4장 개인정보의 안전성 확보조치		제57조(내부관리계획의 수립·시행) 제58조(접근 권한의 관리) 제59조(비밀번호 관리) 제60조(접근통제 시스템 설치 및 운영) 제61조(개인정보의 암호화) 제62조(접속기록의 보관 및 위·변조 사항) 제63조(보안프로그램 설치 및 운영) 제64조(개인정보 점검 및 차단) 제65조(개인정보 파일 및 문서 통제) 제66조(물리적 접근 방지)
제5장 개인정보 영향평가 및 유출대응		제67조(개인정보 영향평가의 대상) 제68조(개인정보의 유출) 제69조(통지시기 및 항목) 제70조(통지방법) 제71조(개인정보 유출신고) 제72조(개인정보 유출대응)

장 구성		조 구성
제6장 영상정보처리기기 설치·운영	제1절 영상정보처리기기의 설치	제73조(적용범위) 제74조(영상정보처리기기 운영·관리 방침) 제75조(관리책임자의 지정) 제76조(사전의견 수렴) 제77조(안내판의 설치)
	제2절 개인영상정보의 처리	제78조(개인영상정보 이용·제 3자 제공 등 제한 등) 제79조(보관 및 파기) 제80조(이용·제3자 제공·파기의 기록 및 관리) 제81조(영상정보처리기기 설치 및 관리 등의 위탁)
	제3절 개인영상정보의 열람 등 요구	제82조(정보주체의 열람 등 요구) 제83조(개인영상정보 관리대장) 제84조(정보주체 이외의 자의 개인영상정보 보호)
	제4절 개인영상정보 보호조치	제85조(개인영상정보의 안전성 확보를 위한 조치) 제86조(개인영상정보처리기기의 설치·운영에 대한 점검)
제7장 개인정보보호 실태점검 및 통합관제센터 운영		제87조(개인정보보호 실태점검) 제88조(개인정보 통합관제센터 운영) 제89조(개인정보 통합관제시스템 연계)
제8장 부칙		제1조(시행일)

자료: 보건복지부(2012.01), 보건복지부 개인정보보호 기본지침.

8. 시사점

이상과 같이 살펴본 국내외 개인정보 보호 관련 법·제도는 내용과 효력, 그리고 적용범위에 있어 점차 강화되고, 확대되고 있으며 자국 내 뿐 아니라 국제적인 교류에 있어서도 상호 적용되는 추세이다. 또한 개인의료정보 보호에 대해서는 의료분야 특성에 맞추어 개인의료정보 보호의 중요성이 더욱 더 부각되어 서비스제공자의 관리책임성 강화, 정보주체의 자기정보에 대한 권리 강화 추세가 반영되고 있으며 통합(omnibus)방식의 법률체계에서도 고시, 지침 등을 통해 점차 상세 규정화하고 있다.

제2절 관련 현황조사

본 절에서는 현재 우리나라에서 개인정보 보호 (관리)현황을 파악하기 위해 주기적으로 실시하고 있는 방송통신위원회 주관의 기업 및 개인 대상 '정보보호실태조사', 공공기관의 개인정보 보호 관리체계 및 침해예방 활동을 자율진단하고 검증하는 안전행정부의 '공공기관 개인정보보호 관리수준 진단', 공공 및 민간부문 중 개인정보 보호 취약분야 및 다량의 개인정보 취급분야 등을 대상으로 하는 안전행정부의 '개인정보보호 현장점검', 그리고 의료기관과 밀접한 관련이 있는 보건복지부 주관의 '보건복지부 소속·산하기관에 대한 개인정보 보호 관리수준 현황조사' 등에 대해 살펴보고 각 조사에 대한 최근결과를 간단히 살펴보았다. 이를 통해 본 연구에서 진행코자 하는 의료기관, 의료인 및 일반국민 대상의 조사에 대한 조사항목 선정 및 향후 개인의료정보 보호관리 현황을 파악하기 위한 주기적인 조사의 필요성 등을 파악하고자 하였다.

1. 정보보호실태조사(기업대상)

국내 민간부문의 개인정보 보호현황을 파악하기 위하여 기업과 개인을 대상으로 2001년부터 매년 실시하고 있는 '정보보호실태조사' 중 기업대상 조사는 기업의 정보보호 및 개인정보 보호현황을 파악하기 위한 조사로 종사자수 5인이상, 네트워크를 사용하는 1대이상의 컴퓨터를 보유하고 있는 전국 사업체를 대상으로 한국인터넷진흥원에서 매년 방문면접조사를 수행하고 있다. 2012년도에는 전체 415,000여 업체 중 5,000여 표본업체를 선정하여 응답기관/응답자, 정보보호기반 및 환경, 정보보호대책, 개인정보보호환경, 개인정보보호 조치, 개인정보침해사고 대응, 개인

정보보호 정책성과평가, 침해사고 피해 및 대응활동 등 8개분야에 걸쳐 조사를 수행하였다(방송통신위원회·한국인터넷진흥원, 2012c, 표 3-11 참조).

〈표 3-11〉 정보보호실태조사(기업) 개요

조사명	구분	내용
2012년 정보보호 실태조사 (기업편) (2012)	조사목적	- 민간 영역에서의 정보보호 인식제고를 위한 각종 정책활동의 성과지표 산출 - 국내 정보보호수준 측정을 위한 각종 지수산출의 지표 데이터 제공 - 국가정보보호백서, 한국인터넷백서등 민간분야 정보보호 통계자료 제공
	주요내용	- 정보보호기반 및 환경 - 정보보호 대책 - 개인정보보호 환경 - 개인정보보호 조치 - 개인정보 침해사고 대응 - 개인정보보호 정책성과평가 - 침해사고 피해 및 대응활동
	조사체계	- 조사대상: 종사자수 5인이상, 네트워크에 연결된 컴퓨터를 1대이상 보유한 전국의 사업체 (전체 415,523개업체 중 5,000개 표본업체 선정) - 조사방법: 방문 면접조사(사업체 전산담당자 및 총무담당자) - 조사기간: 2012.7.20.~2012.9.28. - 조사기관 . 주관기관: 방송통신위원회 . 전담기관: 한국인터넷진흥원 - 법적근거: 정보통신망이용촉진 및 정보보호등에 관한 법률 제52조(한국인터넷진흥원) 제3항, 통계법 제18조(통계작성의 승인)

자료: 방송통신위원회·한국인터넷진흥원(2012c), 2012개인정보보호 실태조사(기업편).

세부 조사항목으로는 먼저 응답기관/응답자분야에서는 사업체의 업종, 규모, 지역, 그리고 응답자 종류에 대한 항목이 포함되어 있다. 다음으로 정보보호기반 및 환경 분야에서는 정보보호정책 및 조직, 정보보호 인식 및 환경, 정보보호교육, 정보보호투자로 구분하고 있으며 정보보호

대책 분야에서는 정보보호시스템 및 서비스도입, 신규서비스도입 및 보안대책, 무선랜, 보안관리로 구분하여 조사항목을 구성하고 있다. 개인정보 보호환경 분야에서는 개인정보수집, 개인정보 보호인식, 개인정보 보호 정책 및 예산으로 개인정보 보호조치 분야에서는 개인정보 보호조치 및 암호화, 보안서버 구축 및 주민번호 대체수단도입, 개인정보 보호 신규제도의 이해 및 준비로 구성하고 있다. 개인정보 침해사고 대응분야에서는 사고경험 및 신고를, 개인정보보호 정책성과평가 분야에서는 정책성과평가 및 홍보효과 측정으로 구분하고 있다. 마지막으로 침해사고 피해 및 대응 분야에서는 피해현황, 침해사고대응관련 문항으로 구성되어 있다(방송통신위원회·한국인터넷진흥원, 2012c, 표 3-12 참조).

〈표 3-12〉 정보보호실태조사(기업) 조사항목

분야	항목	세부항목	
응답기관 및 응답자		조사대상 사업체정보(업종, 규모, 지역)	
		응답자	
정보보호 기반 및 환경	정보보호 정책 및 조직	공식적으로 문서화된 정보보호정책 수립유무	
		정보보호 정책 포함 내용	
		IT관련 책임자의 명시적 임명현황	정보관리책임자(CIO) 임명여부 및 전담여부
			정보보호책임자(CISO) 임명여부 및 전담여부
			개인정보관리책임자(CPO) 임명여부 및 전담여부
		공식적 IT 전담조직 설치 및 운영	공식적인 정보보호전담조직 운영여부
			공식적인 개인정보보호 전담조직 운영여부
	정보보호 인식 및 환경	정보보안 위협 원천별 우려정도	
		경영진의 경영계획 수립 시 정보보호의 중요성 인식정도	
		경영진의 경영계획 수립 시 개인정보보호의 중요성 인식정도	
		직원들의 정보보호 중요성 인식정도(5점척도)	
		직원들의 개인정보보호 중요성 인식정도(5점척도)	
	정보보호 교육	정보보호 교육(개인정보보호교육 포함) 실시여부	
		정보보호 교육 프로그램별 실시현황	CEO등 경영진대상
			정보보호 책임자급직원대상

분야	항목	세부항목		
				IT및정보보호 실무자대상
				컴퓨터사용 일반직원대상
				개인정보관리자대상
				컴퓨터사용 일반직원대상
	정보보호 투자	정보화 투자 대비 정보보호 투자 비율		
		정보보호 예산 증감률(2010년대비 증가 또는 감소)		
		정보보호 관련 지출이 없는 이유		
정보보호 대책	정보보호 시스템 및 서비스 도입	정보보호제품사용현황	네트워크보안	웹방화벽 운영여부
				네트워크(시스템)방화벽 운영여부
				침입방지시스템(IPS) 운영여부
				DDoS차단시스템 운영여부
				통합보안시스템(UTM) 운영여부
				가상사설망(VPN) 운영여부
				네트워크 접근제어(NAC) 운영여부
				무선네트워크보안 운영여부
				모바일보안 운영여부
			시스템보안	PC방화벽 운영여부
				Virus백신 운영여부
				Anti스파이웨어 운영여부
				Anti피싱 운영여부
				스팸차단 SW 운영여부
				보안운영체제 운영여부
			콘텐츠/정보 유출방지보안	DB보안(접근통제) 운영여부
				DB암호 운영여부
				PC보안 운영여부
				보안USB 운영여부
				디지털저작권관리(DRM) 운영여부
			암호/ 인증	보안스마트카드 운영여부
				HW토큰(HSM) 운영여부
				일회용비밀번호(OTP) 운영여부
				공개키기반구조(PK) 운영여부
				통합접근관리(EAM) 운영여부
				싱글사인온(SSO) 운영여부

분야	항목	세부항목		
				통합계정관리(M/IAM) 운영여부
				공인/사설 인증 틀 운영여부
			보안관리	기업보안관리(EMS) 운영여부
				위협관리시스템(TMS) 운영여부
				패치관리시스템(PMS) 운영여부
				자산관리시스템(RMS) 운영여부
				로그관리/분석 틀 운영여부
				취약점분석 틀 운영여부
			기타	기타
		정보보호 업무의 아웃소싱 여부		
		정보보호(보안) 서비스 유형별 아웃소싱 현황		인증서비스 이용여부
				보안관제 이용여부
				보안컨설팅 이용여부
				유지보수 이용여부
				교육훈련서비스 이용여부
				기타
	신규 서비스 도입 및 보안 대책	클라우드 컴퓨팅 서비스 이용현황		
		클라우드 컴퓨팅 서비스 보안대책 수립현황(보안대책확보)		
		클라우드 컴퓨팅 서비스 보안대책 및 가이드라인 내용		서비스제공자 선택시 사업자국적 파악 포함여부
				서비스제공자 데이터처리방침확인 포함여부
				서비스제공자의 개인정보취급방침 확인 포함여부
				공유기능 제공시 개인정보포함화일 공유 금지 포함여부
				개인정보포함화일의 암호화 포함여부
				8자이상 비밀번호설정 및 비밀번호변경 포함여부
				서비스탈퇴시 데이터확인방법 확인 및 완전삭제 포함여부
		클라우드 컴퓨팅 서비스 비이용 이유		
		클라우드 컴퓨팅 서비스 사업자의 보안정책 수립여부		
		클라우드 컴퓨팅 서비스 사업자의 보안정책 내용		서버의 국가위치 명확히 고지 포함여부
				개인정보관련 법규고지 포함여부
				고객이 저장한 데이터처리방침 고지 포함여부
				접근제어기능 구비 포함여부

분야	항목	세부항목	
			신뢰할 수 있는 제3자로부터 주기적으로 개인정보보호기본정책 및 표준이행여부 점검받고 고객에게 결과제공 포함여부
			고객데이터에 임의적으로 접근하지 않고 불가피하게 접근해야할 경우 접근사유 제시 포함여부
			개인정보 및 고객데이터보호조직 운영 및 내부관리계획수립하여 시행 포함여부
			고객이 저장한 개인정보관련자료 이용·변조·훼손 금지 포함여부
			고객의 서비스해지시 고객데이터 완전삭제 포함여부
			개인정보분쟁 발생시 신속하게 대처 가능한 절차마련 포함여부
		모바일 오피스 도입현황	
		모바일 오피스 보안대책 수립현황	
		모바일 오피스 미도입 이유(1,2순위)	
	무선랜	무선랜 구축운영여부	
		무선랜에 대한 보안정책 수립현황	
		무선랜 보안정책 내용	사내 유.무선 네트워크분리운영 포함여부
			전송 데이터보안/암호화적용 포함여부
			무선랜 접근제어/필터링설정 포함여부
			무선랜 접속암호설정 포함여부
			무선랜 통한 SNS 접속차단 포함여부
			주기적인 무선랜 보안점검 포함여부
			무선랜 보안관리팀 및 담당자지정 포함여부
			무선랜 사용자대상 주기적인 보안교육 실시 포함여부
			기타
		외부 상용 무선인터넷서비스 사용가능 여부	
		외부 상용 무선인터넷서비스 보안정책 수립여부	
	보안관리	정기적인 보안점검 수행현황 여부	
		보안패치 적용방법	직원개인용PC
			외부공개 네트워크서버(메일서버, 웹서버등)
			내부이용 로컬서버(파일서버, 프린트서버등)
			정보보호시스템(방화벽, IPS 등)

분야	항목	세부항목	
		사내 정보시스템 사용자 인증방식	사용자 ID/패스워드 사용여부
			일회용비밀번호 사용여부
			소프트웨어 토큰(공인인증서등) 사용여부
			하드웨어 토큰(HSM Hardward Security Module) 사용여부
			바이오인식 사용여부
			기타
		사내 정보시스템 이용 시 차등권한 부여현황	직급별 권한차등관리 사용여부
			직무별 권한차등관리 사용여부
			정규직여부별 권한차등관리 사용여부
			외주업체직원에 대한 권한 제한 사용여부
			기타
			특별한 권한부여하여 관리하지 않음
		주기적인 시스템 로그 및 주요 데이터백업 실시현황	시스템 로그백업실시여부
			주요 데이터 백업실시여부
개인정보보호환경	개인정보수집	이용자(고객) 개인정보 수집방법	
		수집하는 개인정보의 종류	일반정보 수집여부
			가족정보 수집여부
			교육 및 훈련정보 수집여부
			병역정보 수집여부
			부동산정보 수집여부
			소득정보 수집여부
			기타 수익정보 수집여부
			신용정보 수집여부
			고용정보 수집여부
			법적정보 수집여부
			의료정보 수집여부
			조직정보 수집여부
			통신정보 수집여부
			위치정보 수집여부
			신체정보 수집여부
			습관 및 취미정보 수집여부
		보유하고 있는 이용자(고객) 개인정보 규모	

분야	항목	세부항목	
		이용자(고객)의 주민등록번호 수집·이용 여부	
		주민등록번호 수집 목적	회원가입시 본인인증 여부
			중복가입방지 여부
			아이디/패스워드찾기 여부
			고객상담회원관리 여부
			결제 여부
			성인인증 여부
			기타
		주민등록번호 미수집 시 서비스제공에의 영향	
		주민등록번호 미수집 이유	
		개인정보 수집에 대한 인식	개인정보 유출 및 도용가능성은 항상 존재
			웹사이트서비스제공을 위해서는 유출가능성에 상관없이 이용자의 개인정보수집가능
			웹사이트보안이 안정적이면 이용자의 개인정보수집과 이용에 제한을 두지 않아도 됨
	개인정보보호인식	개인정보 항목별 중요도에 대한 인식	일반정보
			가족정보
			교육 및 훈련정보
			병역정보
			부동산정보
			소득정보
			기타 수익정보
			신용정보
			고용정보
			법적정보
			의료정보
			조직정보
			통신정보
			위치정보
			신체정보
			습관 및 취미정보
		개인정보 누출사고 원천에 대한 우려정도	외부로부터 해킹
			내부자에 의한 고의유출
			기업관리 실수로 인한 유출

분야	항목	세부항목	
개인정보보호조치	개인정보보호정책및예산	문서화된 개인정보보호 내부관리계획 수립여부	
		개인정보보호 내부관리계획 내용	개인정보관리책임자 지정 포함여부
			개인정보보호 조직구성, 운영 관련사항 포함여부
			개인정보취급자 교육관련사항 포함여부
			DB시스템 접근권한부여, 변경, 말소 등에 관한 기준수립 및 시행여부
			침입차단시스템 및 침입탐지시스템 설치·운영여부
			비밀번호 생성방법 및 변경주기등 기준설정여부
			개인정보처리시스템 접속일시,처리내역 저장 및 관리 시행여부
			비밀번호 및 바이오정보 일방향 암호화 시행여부
			주민번호 및 계좌정보등 금융정보 암호화 시행여부
			개인정보 송수신시 보안서버 구축 여부
			백신 소프트웨어 설치 및 주기적갱신 및 점검여부
		개인정보보호 예산 배정 여부	
	개인정보보호조치및암호화	개인정보처리시스템 운영 및 관리여부	키보드해킹방지 솔루션 적용 여부
			DB접근내역에 대한 로그저장 여부
			보관하고 있는 개인정보 암호화 저장여부
			USB/이동형 저장장치 통제여부
			노트북, PDA통제여부
		개인정보 암호화 저장 항목	주민등록번호 여부
			계좌번호 여부
			신용카드번호 여부
			비밀번호 여부
			바이오정보 여부
		개인정보 침해사고 예방 및 사후처리 조치내용	개인정보침해사고예방에 관한 매뉴얼 수립여부
			개인정보침해사고 사후 처리방침 수립여부
			개인정보침해발생 징후목록 작성 및 관리여부
			개인정보침해사고로 인한 피해상황 점검 및 증거수집절차 확립여부
			침해사고발생시 내부대응체계 및 보고체계 확립여부
			외부 전문가활용을 위한 비상연락망유지여부
			개인정보피해발생시 개인정보분쟁조정위원회, 개인정보침해신고센터등 관련기관 공지 여부
			기타
			특별한 조치 시행안함

분야	항목	세부항목	
	보안서버 구축 및 주민번호 대체수단 도입	보안서버 도입현황	
		보안서버 구축방식	
		웹사이트 회원 가입 시 본인확인을 위한 방법	
		주민번호 대체수단	i-PIN 여부
			공인인증서 여부
			휴대전화번호, 신용카드번호 여부
			기타(계좌번호 등)
	개인정보보호 신규제도의 이해 및 준비	정보통신서비스 부문 전년도(2011년도) 매출액	
		정보통신망법 개정에 따른 신규제도 인지여부	주민번호수집 이용제한
			개인정보 누출통지 신고제도
			개인정보 유효기간 제도
			개인정보처리시스템 망분리
			개인정보 이용내역 통지제도
			PIMS도입
		신규제도 이행 시 필요한 사항에 대한 의견(1,2순위)	
		신규제도 도입을 위한 준비 정도(복수응답)	
개인정보 침해사고 대응	사고경험 및 신고	개인정보 누출경험여부	
		개인정보 누출사고 유형	외부로부터 해킹
			내부자에 의한 고의누출
			기업의 관리실수로 인한 누출
			기타
		개인정보 누출사고 횟수	
		개인정보 누출사고 규모(개인정보)	
		개인정보 누출사고 인지 시점	
		개인정보 누출사고 발생 시 고지방법(중복응답)	
		개인정보 누출사고 발생 시 주무부처 신고경험유무	
		개인정보 누출사고 발생 시 신고하지 않은 이유	
		개인정보 누출사고 시 보상제공 경험유무	
개인정보 정책성과 평가	정책성과 평가 및 홍보효과 측정	사업자 대상 개인정보보호 교육참석 현황	
		개인정보보호 관련 무료교육 시 참석 의향유무	
		희망하는 개인정보보호 교육 유형(1,2순위)	
		개인정보보호 관련 교육 만족도(5점척도)	
		개인정보 취급자 대상 워크숍 인지여부	
		개인정보 취급자 대상 워크숍 인지경로	

분야	항목	세부항목
		개인정보 취급자 대상 워크숍 참석 여부
		개인정보 취급자 대상 워크샵 인식제고 도움정도(5점 척도)
		개인정보보호 포털사이트 인지여부
		개인정보보호 포털사이트 이용빈도
		개인정보보호 포털사이트 이용내용
		개인정보보호 포털사이트 인식제고 도움정도(5점 척도)
침해사고 피해 및 대응	피해 현황	인터넷 침해사고 유형별 피해 빈도
		정보보안 침해사고 피해사실 인지 시기
		정보보안 침해사고 시 문의 또는 신고경험
		정보보호 피해건수 증감률
		정보보호 피해규모 증감률
		개인정보 유출 및 명의도용으로 인한 피해 현황
	침해사고 대응	정보보안 침해사고 대응을 위한 활동 내용
		현재 수행중인 정보보호활동 평가수단
		침해사고 대응/문제해결을 위한 대외협력채널

자료: 방송통신위원회·한국인터넷진흥원(2012c), 2012개인정보보호 실태조사(기업편).

2012년도 기업부문에 대한 조사결과는 경기침체 등으로 정보보호에 관한 투자가 2011년도 37.2% 대비 전반적으로 감소하였으며(26.1%), 정보보호 예방활동도 감소하고 있는 것으로 나타났다. 한편 개인정보보호 활동은 향상되고 업종별·규모별 정보보호 수준 격차는 심화되고 있는 것으로 나타났다(방송통신위원회, 2013.2.22.).

이러한 '정보보호실태조사'는 5인 이상의 사업체로 제한되어 있고, 사업체 정보에서 업종분류는 OECD의 분류권고안 및 국내통계생산을 위해 13개 업종으로 재분류함에 따라(표 3-13 참조) 의료기관의 경우 종사자 수가 5인 미만인 대부분의 의원급이 포함되지 않고 업종분류에서도 '기타'로 한꺼번에 묶여 분류되어 있어 의료기관에 대한 정보보호 실태현황을 파악할 수 없는 문제점을 지니고 있다.

〈표 3-13〉 정보보호실태조사(기업)에서의 업종분류

한국 표준산업분류 (9차 개정)	정보보호실태조사에서의 업종 분류기준	국제 분류기준
A. 농업, 임업 및 어업	1. 농림수산업(광업포함)	-
B. 광업		
C. 제조업	2. 제조업	제조업(ISIC C)
F. 건설업	3. 건설업	건설업(ISIC F)
G. 도매 및 소매업	4. 도매 및 소매업	도소매업; 자동차 및 모터사이클 수리업 포함(ISIC G)
H. 운수업	5. 운수업	운수업(ISIC H)
I. 숙박 및 음식점업	6. 숙박 및 음식점업	숙박 및 음식점업(ISIC I)
J. 출판, 영상, 방송 통신 및 정보서비스업	7. 출판, 영상, 방송 통신 및 정보서비스업	정보통신업(ISIC J)
K. 금융 및 보험업	8. 금융 및 보험업	-
L. 부동산업 및 임대업	9. 부동산업 및 임대업	부동산업(ISIC L) 사업관리 및 지원서비스업(ISIC N)
M. 전문, 과학 및 기술서비스업	10. 전문, 과학 및 기술서비스업	전문, 과학 및 기술서비스업(M75 수의업 제외)
N. 사업시설관리 및 사업지원 서비스업	11. 사업시설관리 및 사업지원 서비스업	사업관리 및 지원서비스업(ISIC N)
S. 협회 및 단체, 수리 및 기타 개인서비스업	12. 협회, 단체, 수리 및 기타 개인 서비스업	기타 서비스업 (ISIC S,S95 수리업 포함) ISIC S94 협회 및 단체 ISIC S95 컴퓨터, 개인 및 가정용품 수리업 포함 ISIC S96 기타 개인서비스업
D. 전기, 가스, 증기 및 수도사업		
E. 하수·폐기물 처리, 원료 재생 및 환경복원업		
O. 공공행정, 국방 및 사회보장 행정		
P. 교육 서비스업	13. 기타(공공행정, 국방 및 사회보장 행정 제외)	-
Q. 보건업 및 사회복지서비스업		
R. 예술, 스포츠 및 여가관련 서비스업		

자료: 방송통신위원회·한국인터넷진흥원(2012c), 2012개인정보보호 실태조사(기업편).

한편 기업대상의 '정보보호실태조사'는 방문 면접조사로써 그 조사항목이 매우 광범위하고 구체적으로 구성되어 있어, 본 연구에서 진행하고자 하는 온라인조사에는 적용하기 어려운 조사항목이 많았으나 기관의 개인정보 보호 전반에 걸친 조사내용으로 그 중 개인정보 보호환경 분야와 개인정보 보호조치 분야에 대한 항목은 본 연구의 온라인조사에서 활용할 수 있을 것으로 판단된다.

2. 정보보호실태조사(개인대상)

다음으로 개인대상의 정보보호실태조사는 정보보호 및 개인정보보호에 대한 개인의 인식현황, 보안대책현황 등을 파악하기 위해 전국 만 12세~59세이하의 최근 1개월내 인터넷 이용자를 대상으로 하여 한국인터넷진흥원에서 2001년부터 매년 가구방문 면접조사를 수행하고 있다. 2012년도에는 2,500명을 대상으로 조사를 수행하였으며 응답자, 정보보호 및 개인정보보호의 중요성/역기능/심각성에 대한 인식, 정보보호 제품 이용현황 및 정보보호 대책수립 여부, 인터넷침해사고(웜.바이러스, 해킹, 애드웨어.스파이웨어등) 대응현황, 데이터보안을 위한 비밀번호 설정 행태, 신규매체(스마트폰, SNS 무선랜) 보안인식 및 피해예방활동 내용, 개인정보 및 프라이버시침해 방지를 위한 대응활동내용, 인터넷침해사고 및 정보보호관련 인터넷역기능 피해현황 및 신고실태 등을 조사하였다(방송통신위원회·한국인터넷진흥원, 2012b, 표 3-14 참조).

〈표 3-14〉 정보보호실태조사(개인) 개요

조사명	구분	내용
2012년 정보보호 실태조사 (개인편) (2012)	조사목적	- 민간 영역에서의 정보보호인식제고를 위한 각종 정책활동의 성과지표 산출 - 국내 정보보호수준 측정을 위한 각종 지수산출의 지표 데이터 제공 - 국가정보보호백서, 한국인터넷백서등 민간분야 정보보호 통계자료 제공
	주요내용	- 정보보호 및 개인정보보호의 중요성, 역기능, 심각성에 대한 인식 - 정보보호 제품 이용현황 및 정보보호 대책수립 여부 - 인터넷침해사고(웜.바이러스, 해킹, 애드웨어.스파이웨어등) 대응현황 - 데이터보안을 위한 비밀번호 설정 행태 - 신규매체(스마트폰, SNS 무선랜) 보안인식 및 피해예방활동 내용 - 개인정보/프라이버시침해방지를 위한 대응활동내용 - 인터넷침해사고, 개인정보/프라이버시 침해, 불법스팸, 피싱등 정보보호관련 인터넷역기능 피해현황 및 신고실태
	조사체계	- 조사대상: 전국의 만 12~59세이하의 최근 1개월내 인터넷 이용자(2,500명) - 조사방법: 가구방문 면접조사 - 조사기간: 2012.8.20.~2012.9.28. - 조사기관 . 주관기관: 방송통신위원회 . 전담기관: 한국인터넷진흥원 - 법적근거: 정보통신망이용촉진 및 정보보호등에 관한 법률 제52조(한국인터넷진흥원) 제3항

자료: 방송통신위원회·한국인터넷진흥원(2012b), 2012개인정보보호 실태조사(개인편)

먼저 응답자에 대한 세부 조사항목으로는 성, 연령, 학력, 직업, 가구소득, 거주지역이 포함되어 있으며 정보보호 인식과 실천분야는 정보보호 인식현황, 정보보호 관련 정보수집과 실천현황으로 구성하고 있다. 정보화 역기능 대응실태 분야는 정보보호 제품·서비스 이용 및 보안 업데이트, 보안대책 실시현황, 비밀번호 설정 및 관리, 불법스팸 대응, 개인정보/프라이버시 침해대응 항목으로 구성되어 있으며 신규서비스에 대한 정보보호 인식 및 보안대책 분야는 스마트폰 이용·보안, 소셜 네트워크 서비스

이용·보안, 무선랜 이용·보안으로 구성되어 있다. 또한 정보화 역기능 피해현황 분야는 해킹/웜·바이러스/애드웨어/스파이웨어, 개인정보/프라이버시 침해, 피싱 항목으로 구성되어 있으며 마지막으로 정보보호/개인정보보호 성과 평가 분야는 정책 인지 및 효과평가, 홍보 및 캠페인항목으로 구성되어 있다(방송통신위원회·한국인터넷진흥원, 2012b, 표 3-15 참조).

〈표 3-15〉 정보보호실태조사(개인) 조사항목

분야	항목	세부항목
응답자		성, 연령, 학력, 직업, 가구소득, 거주지역
정보보호 인식과 실천	정보보호 인식현황	정보보호의 중요성에 대한 인식
		개인정보보호의 중요성에 대한 인식
		정보화 역기능 유형별 심각성
		개인정보 수집 행태에 대한 인식
		개인정보 유형별 공개에 대한 거부감 정도
		개인정보 관련 권리 인지 상황
		개인정보 관련 동의 정도
	정보보호 관련 정보수집 및 실천현황	정보보호 관련 정보수집 활동
		알고 싶던 정보보호 관련 정보
		정보보호 관련 정보수집의 애로사항
		정보보호를 위한 조치
		개인정보보호를 위한 조치
		서비스 제공자의 정보보호를 위한 조치 실행 정도
		서비스 제공자의 개인정보 보호를 위한 조치 실행 정도
정보화 역기능 대응실태	정보보호 제품·서비스 이용 및 보안 업데이트	정보보호 제품/서비스 이용 현황
		사용하고 있는 정보보호 제품/서비스
		정보보호 제품/서비스 이용 시 활용 기능
		정보보호 제품/서비스를 이용하지 않는 이유
		파일 다운로드 시 바이러스 검사 여부
		바이러스 검사 빈도
		백신 프로그램 업데이트 방법

분야	항목	세부항목
	보안대책 실시현황	현재 실시하고 있는 보안 대책
		운영체제 보안패치 설치 방법
		운영체제 보안패치를 업데이트하지 않는 이유
	비밀번호 설정 및 관리	비밀번호 설정 현황
		비밀번호 설정 및 관리 조치
		비밀번호 변경 주기
	불법스팸 대응	이메일 스팸 방지 조치
		휴대전화 스팸 방지 조치
		본인 운영의 홈페이지/블로그 게시판 스팸 방지 조치
	개인정보/ 프라이버시 침해 대응	온라인 상 개인정보 제공 목적
		개인정보 취급방침 공개 사실 인지 여부
		개인정보 취급방침 확인 여부
		개인정보 취급방침 확인하지 않는 이유
		개인정보 유·노출 예방 및 대응 조치
		인터넷 서비스 회원가입 시 주민번호 이외 수단 인지 여부
		인터넷 서비스 회원가입 시 주민번호 이외 수단 이용 여부
		인터넷 서비스 회원가입 시 주민번호
신규 서비스에 대한 정보보호 인식 및 보안대책	스마트폰 이용·보안	스마트폰 이용 여부
		스마트폰 피해 예방·방지를 위한 조치
		스마트폰 피해 유형별 인지 여부
		스마트폰 이용 시, 보안문제 발생 경로
	소셜 네트워크 서비스 이용·보안	SNS 이용 여부
		SNS 이용 시 피해 인지
		SNS 이용 시 이용수칙 실천 유무
	무선랜 이용·보안	무선랜 이용 여부
		무선랜 피해 방지 조치
		무선랜 보안 조치를 취하지 않은 이유
정보화 역기능 피해현황	해킹, 웜바이러스, 애드웨어· 스파이웨어	정보화 역기능 유형별 피해 경험 및 피해 횟수
		정보보호 관련 피해 신고·상담 경험
		정보화 역기능 피해를 신고하지 않은 이유
	개인정보/ 프라이버시 침해	개인정보/프라이버시 침해로 인한 피해 경험 여부 및 피해 횟수
		개인정보/프라이버시 침해 유형
		개인정보 누출에 대한 인지 경로

분야	항목	세부항목
		개인정보 누출에 대한 희망 대처 방안
		개인정보/프라이버시 침해 피해에 대한 신고 및 문의 여부
		개인정보/프라이버시 침해 신고나 상담하지 않는 이유
		개인정보/프라이버시 침해 사실 통보·고지 받은 경험
	피싱	피싱 경험
		피싱 경험 및 피해
정보보호/개인정보보호 성과평가	정책인지 및 효과 평가	정보보호 관련 정책 인지 및 도움 정도
	홍보 및 캠패인	정보보호 관련 홍보물 접한 경험
		정보보호 관련 홍보물의 도움 정도
		정보보호/개인정보보호 접촉 매체
		정보보호 관련 홍보물 인지 여부
		정보보호 관련 홍보물 접촉 경로
		정보보호 관련 홍보물 도움 정도(세부 캠페인별)

자료: 방송통신위원회·한국인터넷진흥원(2012b), 2012개인정보보호 실태조사(개인편)

2012년도 개인에 대한 '정보보호실태조사' 결과, 정보보호에 대한 인식은 98.7%로 높은 수준을 유지하고 있으나, 정보보호 실천 활동은 전년도 보다 감소한 것으로 나타났다(방송통신위원회, 2013.2.22.).

기업에 대한 '정보보호실태조사'와 마찬가지로 개인에 대한 '정보보호실태조사' 역시 가구 방문 면접조사로 매우 다양한 경로에 대한 인식 및 보호현황과 피해현황에 대해 다루고 있다. 이 중 본 연구에서의 조사에서는 개인정보 보호 관리현황 및 개인정보 보호에 대한 인식을 주로 다룰 예정이므로 개인에 대한 '개인정보보호실태조사'에서의 정보보호 인식현황 항목, 홍보 및 캠페인 항목을 일부 적용하는 한편 역기능에 대한 내용은 주요 내용이 아니므로 역기능 대응실태 및 역기능 피해현황 항목과 같은 역기능에 대한 내용은 다루지 않고자 한다.

3. 안전행정부의 공공기관 개인정보보호 관리수준 진단

안전행정부에서는 지난 2008년부터 중앙행정기관과 지방자치단체 등 공공기관의 개인정보보호 수준향상을 위하여 진단프로그램을 개발·배포하여 1차적으로는 각 기관이 개인정보보호 관리체계 및 침해예방활동 등을 자율진단하고 취약점을 스스로 개선하며, 2차적으로 안전행정부가 진단결과를 검증하는 공공기관 개인정보보호 관리수준 진단 사업을 수행하고 있다(행정안전부 보도자료, 2008.04.03.). 2013년도에는 전체 공공기관의 수준향상을 위해 '12년 대비 101개 기관을 추가하여 진단대상기관을 총 289개 기관으로 확대하였다(안전행정부, 2013, 표 3-16 참조).

〈표 3-16〉 2013년도 공공기관 개인정보보호 관리수준 진단 대상기관 현황

구분	대상기관수		비고
	2012년도	2013년도	
계	188	289	
중앙부처	43	44	기존
광역자치단체	16	17	기존
중앙부처 산하기관	-	50	신규
기초자치단체	-	50	신규
지방공기업	129	128	기존

자료: 안전행정부(2013), 2013년 공공기관 개인정보보호 관리수준진단 계획.

진단지표는 크게 관리체계 구축, 보호대책 수립 및 시행, 침해사고 대책 등 3개 분야로 나누어지며 각 분야에 대해 11개지표 총 23개 세부항목으로 구성되어 있다(안전행정부·한국인터넷진흥원 2013.07., 표 3-17 참조).

2013년도 중앙부처, 광역자치단체, 지방공기업 등 189개 공공기관에 대한 진단결과는 평균 86.54점으로 2012년 평균 89.2점보다 오히려 약간 낮아졌으며, 분야별로는 보호대책 수립은 대체로 양호한 편(91.73점)

이었으나 접근권한 관리, 수탁업체 감독 등 침해사고 예방 및 대응노력(80.65점)은 중점 개선이 필요한 것으로 나타났다. 보건복지부는 44개 중앙부처 중에서 관리체계 구축, 보호대책 수립 및 시행, 침해사고대책 3개부문에서 모두 우수기관으로 결과가 공개되었다(안전행정부, 2013.12.16., 표 3-18 참조).

〈표 3-17〉 2013년도 공공기관 개인정보보호 관리수준 진단 지표현황

분야	지표	세부항목
관리체계 구축	개인정보보호 기반마련	개인정보보호 전담조직과 적정인력에 대한 운영
		개인정보보호 활동 수행을 위한 예산 반영
	위탁업무에 따른 개인정보보호 활동	수탁업체 대상 개인정보처리현황에 대한 관리·감독
		위탁계약에 따른 개인정보처리 시, 법 의무사항에 대한 문서화
	개인정보보호 교육추진	연간 개인정보보호 교육계획 수립
		개인정보취급자, 일반직원 등에 대한 교육 이행
	개인정보 보호책임자의 역할 수행	개인정보 보호책임자 지정 및 역할 정의
		개인정보 보호책임자의 교육 및 관리·감독 역할
보호대책 수립 및 시행	개인정보 이용·제공절차 운영	개인정보에 대한 목적외 이용, 제3자 제공에 따른 절차수립과 이행
		개인정보에 대한 목적외 이용, 제3자 제공시 대장기록 및 관리
	개인정보 파일 관리	개인정보처리방침의 이력관리 및 현행화
		개인정보파일의 등록·변경에 대한 관리
		법에서 정한 개인정보파일 등록항목 여부
	개인정보 영향평가 수행	개인정보 영향평가 수행계획 수립
		개인정보 영향평가 수행
	영상정보처리기기 설치 및 운영	영상정보에 대한 이용·제공·열람 관리대장 운영
		영상정보처리기기 운영·관리방침에 법 의무사항 반영
침해사고 대책	개인정보 노출방지 및 자율개선	개인정보 노출방지를 위한 모니터링, 정기점검 실시, 노출이나 취약점 발견시 후속조치 이행
		개인정보보호 자가진단 참여 및 그 결과에 따른 개선조치 수팽
	개인정보 침해사고 대응절차 수립	개인정보 유·노출 및 침해사고 발생에 대한 대응절차 수립
		대응절차 침해사고 대응체계 구축

분야	지표	세부항목
	개인정보처리시스템의 안전한 이용 및 관리	개인정보처리시스템의 접근권한 관리
		개인정보처리시스템에 대한 접속기록 정기점검 및 후속조치

자료: 안전행정부·한국인터넷진흥원(2013.07), 2013년 공공기관 개인정보보호 관리수준진단 매뉴얼.

〈표 3-18〉 2013년도 공공기관 분야별 개인정보보호 관리수준 진단결과

구분	대상기관수	계(평균)	분야		
			관리체계	보호대책	침해사고대책
전체	189	86.54	86.11	91.73	80.65
중앙부처	44	91.25	90.84	95.67	86.08
광역자치단체(시·도)	17	88.12	89.74	91.19	82.84
지방공기업	128	84.71	84.01	90.42	78.51

자료: 안전행정부(2013.12.16.), 2013년도 공공기관 개인정보보호 관리수준진단 결과 공개, 안전행정부 보도자료.

본 수준진단 조사는 자율진단이 선행되고 공공기관에 적용되는 특징을 가지고 있는 조사로써 개인정보 보호법에 기반하여 안전한 개인정보 보호를 위한 필수항목으로 구성되어 있어 본 연구에서의 조사에 많은 참조 모델이 될 것이나 다만, 개인정보 영향평가 수행과 같은 공공기관에 대한 의무 지표는 적용하지 않고자 한다.

4. 안전행정부의 개인정보보호 현장점검(개인정보보호 실태검사)

기존 정보통신부에서는 2000년 1월부터 시행된 '정보통신망이용촉진 등에 관한 법률'의 개인정보 보호 규정에 의해 정보통신 서비스제공자들에 대한 관련 법규 준수여부를 점검하기 시작하여 이동전화업체, 인터넷 쇼핑몰(머니투데이, 2000.11.3.; 동아일보, 2001.12.26.; 한국경제,

2002.6.17.) 등에 대한 인터넷웹사이트의 규정 준수여부를 점검하였다. 또한 2002년부터는 해당 서비스제공자에 대해 웹사이트 모니터링 뿐 아니라 서면점검, 현장점검 등을 통한 개인정보보호 관련 법규 준부 여부를 점검하여 개선권고 및 과태료 부과 등을 수행해 왔으며(정보통신부, 2007.3.6.) 이후 주관기관이 행정자치부, 행정안전부를 거쳐 현재의 안전행정부에 이르고 있다.

현재 안전행정부에서는 개인정보 침해사고에 대한 범정부차원의 신속한 대응을 위해 2012년 말 정부부처 합동의 '개인정보보호합동점검단'을 구성하여 개인정보 침해사고에 대한 사전 예방관제, 합동 조사점검, 사후 기술지원 및 피해확산 방지 등의 기능을 수행하고 있다(행전안전부 보도자료, 2012.11.9.). '개인정보보호합동점검단'의 현장점검 분야는 개인정보의 수집·이용·제공등, 개인정보의 처리제한, 개인정보의 안전한 관리 등 3개 분야로 나누어진다. 먼저 개인정보의 수집·이용·제공등 분야에 대한 상세 지표로는 개인정보 수집·이용 동의항목, 개인정보 제공 항목, 개인정보 이용·제공 제한 항목, 개인정보 파기항목, 동의방법 항목으로 구성되어 있으며 개인정보의 처리제한 분야에 있어서는 업무위탁에 따른 개인정보 처리제한 항목, 개인정보취급자에 대한 감독 항목으로 구성되어 있다. 개인정보의 안전한 관리 분야에 있어서는 내부관리계획 항목, 접근통제 및 접근권한 제한조치 항목, 암호화항목, 보관 및 위변조 방지 항목, 보안프로그램 설치 및 갱신 항목, 물리적 접근방지 항목, 개인정보처리방침 수립 및 공개항목으로 구성되어 있다(안전행정부 내부자료, 2013, 표 3-19 참조).

'개인정보보호합동점검단'에서는 2013년도에 개인정보 유출이나 침해우려가 있는 취약분야, 다량의 개인정보를 취급하는 분야등을 대상으로 실태검사를 실시하였는 바, 이 중 의료분야에 대해 상반기에는 11개 병원을 대상으로, 하반기에는 11개 의원 및 육아관련업체를 대상으로 하였다[11].

〈표 3-19〉 2013년도 개인정보보호합동점검단의 의료기관대상 실태검사 항목

분야	지표	검사항목	관련 법 조항
개인정보 수집, 이용, 제공등	개인정보 수집·이용 동의	온·오프라인 회원가입, 각종 게시판에서의 개인정보 수집시 동의여부	제15조
		정보주체 동의시 필수 고지항목 적정여부	
	개인정보 제공	개인정보 제3자 제공시 정보주체 동의여부	제17조
		정보주체 동의시 필수고지항목 적정 여부	
	개인정보 이용·제공 제한	개인정보 수집당시 정보주체의 이용·제공동의 범위 초과여부	제18조
	개인정보 파기	목적달성 또는 보유기간 경과후 개인정보 파기여부	제21조
		법 목적에 따른 보유기간 경과후 보관시 별도보관 여부	
	동의받는 방법	고유식별정보, 민감정보 수집시 구분동의 여부	제22조
		재화나 서비스홍보 또는 판매권유시 구분동의 여부	
개인정보 처리 제한	업무위탁에 따른 개인정보 처리제한	수탁사와의 문서에 의한 계약여부	제26조
		수탁사에 대한 교육 및 실태점검 등 관리·감독 여부	
	개인정보취급자에 대한 감독	안전한 개인정보관리를 위한 관리·감독 여부	제28조
		개인정보취급자에 대한 정기적인 교육실시 여부	
개인정보 안전한 관리	내부관리계획 수립·시행	책임자지정, 책임자·취급자 역할, 안전성 조치등	제29조
	개인정보 접근통제 및 접근권한 제한 조치	직급별·업무별 권한 차등부여 및 권한변경기록 3년간 보관여부	
		외부 열람권한이 없는 자에게 공개여부	
		방화벽, IPS 및 VPN 설치여부	
		비밀번호 작성규칙 수립 및 이행여부	
	개인정보 암호화	정보통신망에서 송·수신시 암호화 전송여부	
		인터넷구간, DMZ에 개인정보 저장시 암호화여부	
		내부망 저장시 암호화여부(위험도 분석 등)	
	접속기록 보관 및 위·변조 방지	접속기록 6개월 보관 및 위·변조방지를 위한 접속기록 별도보관 여부	
	보안프로그램 설치 및 갱신	백신소프트웨어 설치 및 갱신여부	
	물리적 접근방지	개인정보의 안전한 보관을 위한 보관시설 마련 또는 잠금장치 설치여부	
	개인정보 처리방침 수립 및 공개	안전성조치 등 개인정보처리방침 반영 여부	제30조

자료: 안전행정부 내부자료(2013)

11) 하반기 실태검사에는 본 연구진도 같이 참여하여 의료기관 현장에서의 애로사항을 확인할 수 있는 기회를 가졌음.

실태조사 결과, 주요 의료기관의 위반 내용은 개인정보 처리 위탁 시 문서에 포함할 사항이 누락되거나 관리감독 소홀, 접속기록 미보관, 전송 저장시 암호화 미조치 등 안전성 확보조치 부실에 관한 것들로 개인정보 관리체계 구축, 개인정보 생명주기에 따른 법규 준수사항 주기적 점검, 개인정보 처리업무 위탁 시 처리사항 문서화, 안전성 확보 조치 및 관리를 위한 접근권한 강화, 암호화 보안프로그램 설치, 개인정보 수집 시 고지사항 고지 등에 관한 개선의 필요성이 부각되었다(메디파나, 2013.07.10.).

본 현장점검 지표는 관련 법에 근거하여 개선권고, 과태료부과 등과 같은 현실적인 점검결과가 나타나므로 기관입장 혹은 의료기관입장에서는 매우 중요한 지표라 할 수 있다. 그러므로 본 연구에서의 조사항목에 가급적 적용하고자 하였다.

5. 보건복지부 소속·산하기관에 대한 개인정보보호 관리수준 현황조사

보건복지부에서는 소속·산하기관의 개인정보 보호활동, 개인정보 취급관리, 기술적 보호조치 등 안전성을 확보하고 개인정보보호에 대한 인식을 제고하고자 2008년부터 매년 개인정보보호 및 관리에 대한 현장점검을 실시하고 있다(보건복지부, 2013a). 현장점검 대상은 2008년 11개에서 2013년 37개로 증가하였으며 소속 및 산하기관 중 점검주기에 따라 매년 실시하는 '가급기관'과, 3년마다 실시하는 '나급기관'으로 분류하고 있다. 점검대상 및 점검항목은 매년 약간씩 차이를 보이고 있다(보건복지부, 2013b, 표 3-20 참고).

〈표 3-20〉 연도별 보건복지부 소속·산하기관에 대한 개인정보보호 관리수준 점검대상 및 점검내용

연도	점검대상		점검내용
'08 (11)	본부	- 공공보건정보, 복지정책DB, 전자바우처, 국가복지, e-보육	개인정보 수집, 이용·제공, 파기 등 처리 주기별 준수사항 이행여부, 개인정보·진료내역 등 대량의 중요·민감 정보의 관리실태, PC 내 개인정보 보유여부 및 관리실태, 개인정보처리시스템의 기술적인 보안대책 적정성
	소속기관	- 질병관리본부, 국가장기이식관리센터	
	소속공공기관	- 국민건강보험공단, 국민연금공단, 건강보험심사평가원, 대한적십자사	
'09 (19)	본부	- 전자바우처, 사회복지시설, 복지정책DB, 보육통합정보, 보건소통합정보	관리적·기술적·물리적 정보보호 현황 점검, 취약점 점검, 조치 지원 및 보호대책 수립, PC내 개인정보 보유여부 및 보안관리 현황, 개인정보 접근로그 분석 및 오남용 사례
	가급	- 소속기관: 질병관리본부 - 산하기관: 국민건강보험공단, 국민연금공단, 건강보험심사평가원, 대한적십자사	
	나급	- 소속기관: 국립서울병원 - 산하기관: 국립장기이식관리센터, 국립중앙의료원, 국립암센터, 한국노인인력개발원, 한국보건의료인국가시험원, 한국보건산업진흥원, 대한결핵협회, 한국보건복지인력개발원	
'10 (12)	가급	- 산하기관: 건강보험심사평가원, 국민건강보험공단, 국민연금공단, 대한적십자사, 국립암센터	개인정보보호 현황, 정보시스템 취약점 관리, 업무용 PC 내 개인정보 관리, 개인정보처리시스템 접근로그 분석, '10년도 국정감사 시 개인정보보호 관련 지적 사항 이행여부
	나급	- 소속기관: 국립부곡병원, 국립마산병원, 국립소록도병원, 국립재활원 - 산하기관: 한국보건복지정보개발원(행복e음시스템), 한국사회서비스관리원(전자바우처시스템, 보육통합정보시스템), 한국사회복지협의회	
'11 (14)	가급	- 소속기관 : 질병관리본부 - 산하기관 : 국민건강보험공단, 건강보험심사평가원, 국민연금공단, 대한적십자사, 한국보건복지정보개발원, 국립암센터	개인정보보호 현황, 정보시스템 취약점 관리, 업무용 PC 내 개인정보 관리, 개인정보처리시스템 접근로그 분석, 개인정보 보호법 대비사항
	나급	- 소속기관: 국립목포병원, 국립나주병원, 국립춘천병원, 국립공주병원 - 산하기관: 한국장애인개발원, 한국국제보건의료재단, 국립중앙의료원	

연도	점검대상		점검내용
’12 (29)	본부	- 행복e음, 보건소통합정보, 보육통합정보, 전자바우처, 사회복지시설정보, 독거노인응급안전돌보미, e하늘장사종합	개인정보 보호법 준수 정도 종합 평가, 업무용 PC 내 개인정보 관리, 개인정보처리시스템 취약점 ※ 의료원 개인정보관리 현장점검 실시는 3개 분야(개인정보보호정책환경, 개인정보처리, 개인정보 침해대응), 18개 지표임.
	가급	- 소속기관: 질병관리본부 - 산하기관: 한국보건복지정보개발원, 국민건강보험공단, 국민연금공단, 건강보험심사평가원, 대한적십자사, 국립암센터, 국립중앙의료원	
	나급	- 소속기관 : 국립서울병원, 오송생명과학단지지원센터, 국립망향의동산 - 산하기관: 한국보건인국가시험원, 한국보건복지인력개발원, 한국보건산업진흥원, 한국건강증진재단, 한국보육진흥원, 한국노인인력개발원 ※ 의료원: 천안의료원, 충주의료원, 경기의료원(수원병원) 인천의료원, 서울의료원	
’13 (37)	본부	- 행복e음, 보건소통합정보, 보육통합정보, 전자바우처, 사회복지시설정보, 독거노인응급안전돌보미, e하늘장사종합	개인정보보호 관리체계 구축현황 개인정보보호대책 수립 및 시행현황, 침해사고 대책마련, 개인정보 처리현황, PC 개인정보보호현황, 안전성 확보 조치 현황
	가급	- 소속기관: 질병관리본부 - 산하기관: 국민건강보험공단, 국민연금공단, 건강보험심사평가원, 대한적십자사, 국립암센터, 한국보건복지정보개발원, 국립중앙의료원	
	나급	- 소속기관: 국립서울병원, 국립나주병원, 국립부곡병원, 국립춘천병원, 국립공주병원, 국립소록도병원, 국립망향의동산관리소, 국립재활원, 국립마산병원, 국립목포병원, 오송생명과학단지지원센터 - 산하기관: 한국보건산업진흥원, 한국보건복지인력개발원, 한국보건의료인국가시험원, 한국국제보건의료재단, 한국사회복지협의회, 한국노인인력개발원, 한국장애인개발원, 한국보육진흥원, 한국건강증진재단, 한국보건의료연구원(’13년 신규), 한국의료분쟁조정중재원(’13년 신규)	

자료: 보건복지부(2013b), 보건복지부 내부자료.

2013년도 점검분야 및 항목으로는 관리체계 구축, 보호대책 수립 및 시행, 침해사고 대책, 개인정보처리, PC개인정보보호, 안전성 확보조치 등 6개 분야로 나누어 18개 지표, 총 52개 진단항목으로 구성되어 있다 (표 3-21 참조).

〈표 3-21〉 2013년도 보건복지부 개인정보보호 관리수준 현황조사를 위한 진단지표 및 진단항목 현황

분야	지표	진단항목	관련 법 조항
관리 체계 구축	1. 개인정보보호 기반마련	1.1 개인정보보호 전담조직 및 인력에 대한 구성·운영	제31조
		1.2 개인정보보호 예산 책정	제10조
	2. 위탁업무에 따른 개인정보보호 활동	2.1 수탁업체대상 개인정보 처리현황에 대한 관리·감독	제26조
		2.2 위탁계약시 법 의무사항에 대한 문서화	제26조
		2.3 위탁사실에 대한 홈페이지등 공개	제26조
		2.4 재화 또는 서비스에 대한 홍보, 판매권유에 대한 업무위탁시 정보주체에게 서면, 전자우편, 전화등의 방법으로 고지	제26조
	3. 개인정보보호 교육 추진	3.1 연간 개인정보보호 교육계획 수립	제31조
		3.2 개인정보취급자, 일반직원등에 대한 교육 이행	제28조 제31조
	4. 개인정보 보호책임자 역할 수행	4.1 개인정보 보호책임자의 역할 정의	제31조
		4.2 개인정보 보호책임자가 교육이수 및 관리·감독 등 역할 수행	제26조 제28조 제31조
보호 대책 수립 및 시행	5. 개인정보 목적 외 이용·제3자 제공절차 운영	5.1 개인정보를 목적외 이용하거나 제3자제공에 따른 절차 수립 및 이행	시행령 제15조
		5.2 개인정보를 목적외 이용하거나 제3자제공시 대장기록 및 관리	제18조
		5.3 개인정보를 목적외 이용하거나 제3자제공시 타당한 근거확보	제17조 제18조
		5.4 개인정보를 제3자제공시 안전한 방법으로의 제공	제18조
		5.5 개인정보를 타 기관에 연계/제공시 문서요청 및 문서수령	제18조

분야	지표	진단항목	관련 법 조항
	6. 개인정보 처리방침	6.1 개인정보처리방침 공개 및 법의무사항에 대한 반영	제30조
		6.2 정보주체의 개인정보 열람, 정정삭제, 처리정지권리 보장 및 요청에 따른 처리기간 준수, 대응	제4조 제35조
	7. 개인정보파일 관리	7.1 개인정보파일 생성.변경 시 60일이내등록	시행령 제34조
		7.2 개인정보파일 보유기간 산정시 개인정보처리에 필요한 최소기간 적용	표준 지침 제64조
		7.3 개인정보파일 등록항목 전체 등록	제32조
	8. 개인정보영 향평가(PIA) 수행	8.1 개인정보영향평가 수행계획 수립	제33조
		8.2 개인정보영향평가 수행계획에 따른 이행	제33조
	9. 영상정보 처리기기 설치 및 운영	9.1 개인영상정보 이용·제공, 파기, 열람시 해당내용에 대한 기록 및 관리	시행령 제25조
		9.2 개인영상정보 분실·도난·유출·변조 또는 훼손되지 않도록 안전성확보 조치	시행령 제25조
		9.3 영상정보처리기기 운영·관리방침에 법 의무사항 반영	제25조
		9.4 영상정보처리기기 운영시 영상정보처리기기 운영·관리방침 수립 및 홍페이지 공개	시행령 제25조
		9.5 영상정보처리기기의 녹음기능 및 임의조작 금지	제25조
		9.6 영상정보처리기기 설치장소에 안내판설치	제25조
		9.7 영상정보처리기기 신규설치시 사전의견수렴, 위탁시 문서수신, 열람·제공·파기에 따른 기록관리수행 등 영상정보처리기기의 적절한 운영	제25조
침해 사고 대책	10. 개인정보 노출방지	10.1 개인정보 노출방지를 위한 보안시스템 및 백신소프트웨어 설치, 운영	제29조
	11. 개인정보 침해사고 대응절차	11.1 개인정보 유·노출 및 침해사고 발생에 대한 대응절차 수립	제34조
		11.2 대응절차를 개인정보취급자에게 전파하여 신속하게 대응할 수 있는 체계 구축	제34조
	12. 개인정보처리 시스템 접근권한 및 접속기록	12.1 개인정보처리시스템 접근권한에 대한 담당자별 차등부여	고시 제4조
		12.2 전보·퇴직 등의 권한변동 사유 발생시 즉각적인 권한의 변경·말소조치 이행	고시 제4조
		12.3 개인정보처리시스템의 접근권한 부여·변경·말소기록에 대한 최소3년 이상 보관절차 마련 및 실행	시행령 제30조

분야	지표	진단항목	관련 법 조항
		12.4 개인정보처리시스템에 대한 접속기록 점검·후속조치, 보관·관리 등 자발적이고 충실한 관제활동	제29조
		12.5 접근통제시스템 설치·운영	제29조
개인정보처리	13. 수집동의	13.1 정보주체로부터 개인정보 수집시 법적근거 마련	제15조
		13.2 정보주체의 개인정보 수집시 필수항목(수집목적, 수집항목, 보유및이용기간, 동의거부 권리 및 거부시 불이익)에 대한 안내 및 동의 수행	제15조 제16조
		13.3 정보주체가 최소한의 정보외 부가적인 개인정보수집에 동의하지 않아도 재화 또는 서비스제공이 가능한 지침또는방침	제16조 제22조
		13.4 만 14세미만 아동의 개인정보 수집시 법정대리인의 동의	제22조
		13.5 개인정보 수집시 별도의 동의가 필요한 사항(고유식별정보, 민감정보)에 대한 별도의 동의	제17조 제18조 제23조 제24조
		13.6 개인정보 보호법 시행령에 의한 대체가입수단(I-PIN, 신용카드, 공인인증서, 휴대폰/유선전화) 의무도입 대상자의 경우 대체가입수단 제공	제24조
	14. 개인정보 파기 및 관리	14.1 개인정보 처리목적 달성 및 보유기간 경과시 복원이 불가능한 방법으로 파기	제21조
		14.2 개인정보파일 파기시 안행부에 파기사실에 대한 등록 및 파기관리대장 작성·관리	제21조
PC 개인정보보호	15. PC 개인정보보호	15.1 보안프로그램 설치 및 정기적인 업데이트	제29조
		15.2 PC에 저장된 개인정보의 경우, 별도의 암호화 혹은 보안 USB 저장	제29조
안전성확보조치	16. 암호화	16.1 고유식별 정보, 바이오정보, 비밀번호의 암호화	제24조 제29조
		16.2 고유식별정보, 바이오정보, 비밀번호를 보조저장매체 혹은 정보통신망을 통해 송·수신 시 암호화	제24조 제29조
	17. 비밀번호	17.1 비밀번호 작성규칙 수립 및 준수	제29조
	18. 출입통제	18.1 개인정보처리구역에 대한 비인가자의 출입통제 및 출입에 따른 이력관리 실시	제29조
		18.2 개인정보 기록문서 및 보조저장매체 보관시 잠금장치가 설치된 장소 보관	제29조

자료: 보건복지부(2013b), 보건복지부 내부자료.

보건복지부 소속·산하기관에 대한 개인정보보호 관리수준 현황조사 지표는 안전행정부의 공공기관 개인정보보호 관리수준 진단지표를 기반으로 하여 보건복지부 업무의 특성을 반영한 것으로 상대적으로 매우 상세한 항목으로 구성되어 있다. 그러므로 본 연구에서의 조사항목 선정에 있어 이 중 의료기관의 특성을 반영할 수 있는 항목들을 고려하고자 하였다.

6. 시사점

이상과 같은 관련 현황조사를 살펴본 결과, 우리나라에서는 현재 보건복지부문, 의료기관에 대한 개인정보보호 관리실태와 더불어 개인의료정보 보호에 대한 인식수준을 파악할 수 있는 주기적인 조사는 없는 실정이다. 개인정보 보호에 대한 필요성과 중요성에 의해 개인정보보호 실태조사가 기업단위, 개인단위로 매해 실시되고는 있으나 앞에서 언급한 바와 같이 종사자수가 5인 미만인 대부분의 의원급이 포함되지 않고, 의료기관에 대한 별도의 분석자료가 산출되지 않으며 개인의료정보 보호에 대한 적합한 항목이 포함되어 있지 않아 정확한 실태파악이 어려운 상황이다. 그러므로 향후 보건복지부문, 의료기관에 적용가능한 개인(의료)정보 보호에 대한 실태조사가 주기적으로 수행되어 이에 대한 문제점을 파악하여 차별화되고 현실적인 대책마련이 필요하다 하겠다.

제3절 관련 인증제도[12)]

개인정보 유노출, 오남용 등을 막기 위해 국가적 차원의 법제화와 더불어 중요한 것이 민간차원의 자율규제적 측면에서의 인증제이다. '개인정보 보호 인증'은 기관의 개인정보 보호를 위한 일련의 조치와 활동이 특정 기준에 부합됨을 승인하는 것[13)]으로 국내에서 개인정보 보호와 관련하여 추진하고 있는 인증제도는 기관 홈페이지에 대한 것과 기관의 개인정보 보호 관리체계에 관한 것으로 양분될 수 있다. 이에 본 절에서는 이러한 국내의 개인정보 보호관련 인증제도와 더불어 우리나라 개인정보 보호체계와 매우 비슷한 일본의 인증제도인 P 마크제도, 그리고 개인정보 보호관련 인증제도는 아니지만 의료기관에서의 의료서비스 질 향상 측면에서의 개인정보 보호 항목이 포함되어 있는 의료기관 인증제에 대한 내용과 그 현황에 대해 살펴보고자 한다.

먼저 기관 홈페이지에 대한 인증제도는 개인정보 보호의 안전성 확보를 위해 미리 정해놓은 기준에 도달 시 특정 마크(Mark)를 부여하는 것으로, 민간단체인 개인정보보호협회(OPA, Online Privacy Association) 정보보호마크 인증위원회가 주관하는 '개인정보 보호마크(ePRIVACY Mark)'와 '인터넷사이트 안전마크(i-Safe Mark)'가 있다. 한편 기관의 전반적인 개인정보 보호 관리체계의 수준을 확인하는 제도로는 '개인정보보호 관리체계 인증제도(PIMS, Personal Information Management System)', '개인정보 영향평가 제도(PIA, Privacy Impact Assessment)', '개인정보 보호수준 인증제도(PIPL, Personal Information Protection Level)'가 있으며, '일본의 P 마크

12) 본 절은 정영철·이야리(2013.11.) 원고에 일부 내용을 추가하여 재작성함.
13) 개인정보 보호 인증제 운영에 관한 규정 제2조.

제도', 그리고 우리나라 '의료기관 인증제도'를 사례로 살펴봄에 의의가 있다 하겠다.

1. 홈페이지 개인정보보호 인증마크제도[14)]

우리나라에서 홈페이지에 대한 개인정보 보호 인증마크제도는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 및 '개인정보 보호법'(공공기관)에 근거하여 시행되고 있는 민간자율적 인증마크제도로 개인정보보호협회(OPA: Online Privacy Association) 정보보호마크인증위원회가 주관하고 있다.

인증대상은 기업 혹은 기관의 홈페이지(인터넷사이트)로, 인증마크에는 개인정보보호마크(ePRIVACY Mark)와 인터넷사이트안전마크(i-Safe Mark) 두가지가 있다. 이중 개인정보보호마크(ePRIVACY Mark)는 생명주기, 관리과정, 보호대책 등 3개 분야에 대한 세부기준을 적용하여 2000년부터 시행하고 있으며 일정수준이상을 획득한 기관 사이트에 인증마크를 부여하고 있다. 또한 인터넷사이트안전마크(i-Safe Mark)는 생명주기, 관리과정, 보호대책, 정보보호대책, 소비자보호 등 5개 분야에 대한 세부기준을 적용하여 2002년부터 시행하고 있다(표 3-22 참조).

14) 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20.].

〈표 3-22〉 국내 홈페이지 개인정보보호 인증마크 심사기준

구분	분야	영역	통제 항목수	세부통제 항목수	점검 항목수
ePIVACY	생명주기	1. 개인정보 수집	4(4)	6(6)	13(15)
		2. 개인정보 수집의 특별조치	2(2)	2(2)	4(4)
		3. 개인정보의 이용	4(4)	5(6)	11(14)
		4. 개인정보의 파기	2(2)	3(3)	7(8)
	관리과정	1. 이용자의 권리	2(2)	4(4)	10(11)
		2. 공개 및 책임	3(3)	3(3)	9(9)
		3. 주민등록번호(고유식별번호) 처리	1(1)	2(2)	4(4)
	보호대책	1. 개인정보의 안전성 확보를 위한 기술적, 관리적 보호조치	5(7)	11(12)	25(29)
		2. 개인정보의 안전성 확보를 위한 물리적 보호조치	2(2)	2(2)	3(4)
	합계		25(27)	38(40)	86(98)
i-Safe	생명주기	1. 개인정보 수집	2(3)	4(4)	7(6)
		2. 개인정보 수집의 특별조치	1(1)	1(1)	2(2)
		3. 개인정보의 이용	4(3)	5(5)	11(11)
		4. 개인정보의 파기	2(1)	3(1)	7(3)
	관리과정	1. 이용자의 권리	2(2)	3(2)	8(6)
		2. 공개 및 책임	3(3)	3(3)	7(7)
		3. 주민등록번호(고유식별 번호) 처리	0(1)	0(1)	0(3)
	보호대책	1. 개인정보의 안전성확보를 위한 기술적, 관리적 보호조치	2(3)	3(4)	7(10)
	정보보호대책(시스템보호)	1. 보완과 신뢰성 확보를 위한 물리적 요건	6(6)	7(7)	12(12)
		2. 보완과 신뢰성 확보를 위한 기술적 요건	10(10)	11(11)	21(21)
		3. 보완과 신뢰성 확보를 위한 관리적 요건	9(9)	16(6)	41(41)
	소비자보호	1. 소비자보호	2(0)	5(0)	13(0)
	합계		43(41)	61(44)	136(122)

주: 민간기업 심사기준. 단, ( )항목은 공공기관 심사기준
자료: 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20.]

두 개 마크에 대한 유효기간은 모두 1년이며 2013년 10월현재, 개인정보보호마크(ePRIVACY Mark)가 유효한 사이트는 138개, 인터넷사이트안전마크(i-Safe Mark)가 유효한 사이트는 58개, 두 개 마크가 모두 유효한 사이트는 39개로 총 157개 사이트에 ePRIVACY Mark 혹은 i-Safe Mark가 유효하게 부여되어 있다(표 3-23 참조).

〈표 3-23〉 국내 홈페이지 개인정보보호 인증마크 부여(유효) 현황(2013년 10월 현재)

구분	사이트 수
ePRIVACY 유효	138
i-Safe 유효	58
ePRIVACY와 i-Safe 동시 유효	39

자료: 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20.] .

이러한 인증마크 취득 시에는 심사기준 변경부분에 대한 재인증심사 실시, 사후모니터링, 개인정보보호 우수성에 대한 홍보효과, 고가의 컨설팅 대비 비용절감, 개인정보보호관련 전문교육 기회획득, 정보보호관련 수상에서의 가산점 획득, 탬플릿 획득을 통한 개인정보관리계획 수립 용이 등과 같은 기대효과를 꾀하고 있다.

한편 현재 유효한 사이트 중 의료기관을 살펴본 결과 서울대학병원 1개소만이 홈페이지 개인정보보호 인증마크(ePRIVACY와 i-Safe 동시에 유효)를 획득하고 있어 우리나라 의료기관의 경우 개인정보 보호를 위한 자율규제적인 참여에 보다 많은 노력을 기울여야 할 필요성이 제기되고 있다.

2. 개인정보 보호 관리체계 인증제도(PIMS, Personal Information Management System)

PIMS 인증제도는 '개인정보보호 관리체계 인증 등에 관한 고시(방송통신위원회 고시 제2013-17호)'에 따른 기준의 적합성을 인증하는 제도로 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조의3(개인정보보호 관리체계의 인증), 그리고 동법 시행령 제54조의2(개인정보보호 관리체계의 인증)에 근거하여 정보통신사업자를 대상으로 하고 있다.

본 제도는 방송통신위원회 주관 하에 한국인터넷진흥원이 인증기관으로서 2010년부터 시행하고 있으며 정보통신망에서 개인정보보호활동을 체계적이고 지속적으로 수행하기 위해 필요 기준에 맞는 관리적, 기술적, 물리적 보호조치를 포함한 개인정보보호 관리체계를 수립·운영하고 있는 기관에 인증을 부여한다.

이러한 PIMS 인증심사는 서면 및 현장심사를 병행하며 인증기준은 '개인정보보호 관리과정', '개인정보 보호대책', 그리고 '생명주기' 등 3개분야 총 124개 점검항목으로 구성하고 있다. '개인정보보호 관리과정'에서는 개인정보 보호를 체계적, 주기적으로 수행하고 있는지에 대해 점검하며 '개인정보 보호대책'에서는 개인정보 보호를 위한 관리적, 물리적, 기술적 보호조치를 점검한다. 또한 '생명주기'에서는 개인정보 생성에서 파기까지에 대한 법률준수 여부를 점검하고 있다(개인정보 보호 관리체계 인증 등에 관한 고시, 표 3-24 참조).

PIMS인증에 대한 유효기간은 3년으로 PIMS 인증서는 2010년 시행이후 2013년 10월 현재까지 총 29개 사업자에게 발급되었다. 이러한 PIMS 인증 취득 시 인센티브로는, 해당 기업에서 개인정보 사고 발생시 과징금 및 과태료 경감, 심사기준 변경부분에 대한 재인증심사 실시, 사

후모니터링, 해당 기업에 대한 개인정보보호 우수성 홍보효과, 고가의 컨설팅 비용 대비 비용절감, 개인정보보호관련 전문교육 기회획득, 정보보호관련 수상에서의 가산점 획득, 템플릿 획득을 통한 개인정보관리계획 수립 용이 등과 같은 기대효과를 꾀하고 있다(정보보호 및 개인정보보호 관리체계 인증 사이트, [인용 2013.10.20.]).

〈표 3-24〉 개인정보 보호 관리체계 인증심사 기준

분야	영역		통제목적		점검 항목수
계					124
개인정보보호 관리과정	1	개인정보보호 정책수립 및 범위설정	1.1	개인정보보호정책 수립	1
			1.2	범위설정	1
			1.3	개인정보 흐름파악	1
	2	경영진 책임 및 조직구성	2.1	경영진 참여	1
			2.2	개인정보보호 조직 구성 및 자원 할당	1
	3	위험관리	3.1	위험관리 방법 및 계획 수립	1
			3.2	위험 식별 및 평가	1
			3.3	개인정보보호대책 선정 및 이행계획 수립	1
	4	개인정보보호 대책 구현	4.1	개인정보보호대책의 효과적 구현	1
			4.2	내부 공유 및 교육	1
	5	사후관리	5.1	법적 요구사항 준수검토	1
			5.2	개인정보보호 관리체계 운영현황 관리	1
			5.3	내부감사	1
개인정보 보호대책	1	개인정보 보호정책	1.1	정책의 승인 및 공표	2
			1.2	정책의 체계	2
			1.3	정책의 유지관리	2
	2	개인정보 보호조직	2.1	조직체계	4
			2.2	역할 및 책임	2
	3	개인정보 자산분류	3.1	개인정보의 식별 및 책임	1
			3.2	개인정보의 분류 및 취급	1

분야	영역		통제목적		점검 항목수
	4	교육 프로그램 수립	4.1	교육계획	3
			4.2	교육 시행 및 평가	1
	5	인적보안	5.1	개인정보 취급자 관리	4
	6	침해사고관리	6.1	절차 및 체계	2
			6.2	대응 및 복구	3
			6.3	사후관리	2
	7	기술적 보호조치	7.1	접근통제	14
			7.2	암호통제	2
			7.3	운영통제	11
			7.4	매체보안	2
			7.5	시스템 개발보안	7
			7.6	접속기록 관리 및 모니터링	4
			7.7	출력, 복사 통제	1
			7.8	개인정보표시 제한	1
	8	물리적 보호조치	8.1	보호구역	5
			8.2	사무실보호	2
			8.3	영상정보처리기기 보안	1
생명주기	1	개인정보 수집에 따른 조치	1.1	최소한의 정보수집	5
			1.2	개인정보 수집시 고지 및 동의획득	3
			1.3	개인정보 취급방침	1
	2	개인정보 이용 및 제공에 따른 조치	2.1	동의범위내 개인정보 사용	1
			2.2	이용자 권리보호	6
			2.3	외부 위탁시 개인정보 보호	4
			2.4	제3자 제공시 개인정보 보호	3
			2.5	개인정보 이전시 개인정보 보호	2
	3	개인정보 관리 및 파기에 따른 조치	3.1	개인정보 관리 및 파기	6
로고					

자료: 개인정보보호 관리체계 인증 등에 관한 고시(방송통신위원회 고시 제2013-17호).

3. 개인정보 보호수준 인증제도(PIPL, Personal Information Protection Level)

PIPL 인증제도는「개인정보 보호법」제13조 제3호 '개인정보 보호 인증마크의 도입·시행 지원'에 따라 도입하게 된 제도로써, 2013년 10월 제정·고시된 '개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45호)'에 근거하고 있다[15].

본 제도는 안전행정부 주관 하에 한국정보화진흥원이 인증에 관한 업무를 수행하며(인증기관) 인증기준은 '개인정보보호 관리체계', '개인정보 보호 대책구현' 2개분야 총 65개 심사항목으로 구성하고 있다. 대상기관은 규모와 특성에 따라 대기업·공공기관, 중소기업, 소상공인용 등 3개 유형으로 구분되며 인증 유효기간은 3년이다(개인정보 보호 인증제 운영에 관한 규정, 표 3-25 참조).

한편, 정부(안전행정부)는 PIPL 인증 취득 시 '개인정보 보호법'에 따라 실시되는 기획점검 대상에서 제외 혹은 점검 유예, 고의성 없는 위반사항에 대한 과태료 등 행정처분 감경, 개인정보보호 교육기회 부여, 개인정보보호 우수기관에 대한 포상 실시 등과 같이 다양한 정책적 지원을 계획하고 있다(안전행정부, 2013.10.28.).

본 제도는 개인정보 보호를 위한 규제측면의 개인정보 보호법 시행과 더불어 자율규제적인 측면의 인증제도 시행에 있어 그 대상을 가장 광범위하게 넓힌 것으로 앞으로 많은 기관이 취득하기 위해서는 보다 다양하고 효과적인 인센티브 정책이 필요하리라 생각된다.

---

15) 2013년 11월 28일부터 인증심사 신청.

〈표 3-25〉 PIPL 인증 심사기준

분야	영역		심사목적		심사 항목수
개인정보보호 관리체계	1	보호체계의 수립	1.1	관리계획	2
			1.2	조직	1
			1.3	경영진의 책임	2
	2	실행 및 운영	2.1	문서화	1
			2.2	개인정보 식별	1
			2.3	위험관리	4
	3	검토 및 모니터링	3.1	개인정보보호체계의 검토 및 모니터링	2
	4	교정 및 개선	4.1	교정 및 개선활동 실적관리	1
			4.2	내부 공유 및 인식제고	1
개인정보보호 대책구현	1	개인정보 처리제한	1.1	개인정보 수집시 보호조치	7
			1.2	개인정보 이용 및 제공시 보호조치	3
			1.3	개인정보의 보유시 보호조치	2
			1.4	개인정보 파기시 보호조치	2
	2	정보주체 권리보장	2.1	권리보장	3
	3	관리적 안전성 확보조치	3.1	개인정보 보호책임자의 지정	1
			3.2	교육 및 훈련	2
			3.3	개인정보취급자 관리	2
			3.4	위탁업무관리	3
			3.5	개인정보 유출사고 대응	2
	4	기술적 안전성 확보조치	4.1	접근권한 관리	3
			4.2	접근기록 관리	2
			4.3	운영보안	7
			4.4	암호화 통제	2
			4.5	개발보안	2
	5	물리적 안전성 확보조치	5.1	영상정보처리기기 관리	2
			5.2	물리적 보안관리	5

로고				
	 인증2013-○○○○ 인증범위:_____ 〈 유형3(공공기관용) 〉	 인증2013-○○○○ 인증범위:_____ 〈 유형3(대기업용) 〉	 인증2013-○○○○ 인증범위:_____ 〈 유형2(중소기업용) 〉	 인증2013-○○○○ 인증범위:_____ 〈 유형1(소상공인용) 〉

자료: 개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45호).

4. 개인정보 영향평가제도(PIA, Privacy Impact Assessment)

'개인정보영향평가'란 개인정보를 취급하는 사업 시행이 국민의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 개선방안을 도출하는 절차로(개인정보영향평가사이트, [인용 2013.10.20.]) 공공기관의 경우에는 특정기준[16]에 해당하는 개인정보파일을 운영하는 경우 이를 수행하여야 하며, 수행 후 그 결과를 안전행정부장관에게 제출하여야 한다. 공공기관 외 개인정보처리자는 개인정보 침해가 우려되는 경우 개인정보영향평가를 위한 노력을 권장하고 있다(개인정보 보호법 제 33조).

우리나라에서 개인정보영향평가가 시행된 것은 2005년부터이며 개인

16) 개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상)
① 구축·운용또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
④ 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

정보 보호법 시행인 2011년부터 법적 의무화가 시행되었다. 이러한 PIA 제도는 '개인정보 보호법' 제33조(개인정보 영향평가) 및 동법 시행령 제35조(개인정보 영향평가의 대상)에 근거하여 공공기관은 시행령에 의한 개인정보파일[17]의 운용으로 정보주체의 개인정보 침해가 우려되는 경우, '개인정보 영향평가에 관한 고시(행정안전부고시 제2012-59호)'에 의한 기준에 따라 그 위험요인을 분석하고 개선사항을 도출하기 위한 평가를 수행하게 하고 있다. 공공기관 외 민간의 경우에는 개인정보 침해 우려시 개인정보영향평가를 위한 노력을 권장하고 있다.

의무수행 대상 시스템의 경우 안전행정부장관으로부터 지정받은 개인정보 영향평가기관에 의뢰하여 영향평가를 수행하고 그 결과를 안전행정부 장관에게 제출하도록 되어 있다. 2011년부터 2012년 3월현재까지 지정받은 개인정보 영향평가기관은 (주)한국정보기술단, 인포섹(주), 금융결제원, 시큐베이스(주), (주)엘지 씨엔에스, 한국아이비엠(주)등 모두 18개기관[18]이 있다

PIA의 평가분야는 대상기관의 개인정보보호 관리체계, 대상시스템의 개인정보보호 관리체계, 개인정보 처리단계별 보호, 특정 IT기술 활용시 개인정보보호 등 크게 4개 분야로 나누어 18개영역 총 120여개 항목으

17) 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

18) 개인정보 영향평가기관 지정 공고, 행정안전부 공고 제2011-416호;
개인정보 영향평가기관 지정 공고, 행정안전부 공고 제2012-61호.

로 구성되어 있다(행정안전부·한국인터넷진흥원, 2012, 표 3-26 참조).

본 제도는 특정기준에 의한 공공기관의 경우 의무화하고 있어 자율규제적인 측면과 동시에 규제적인 측면을 동시에 지니고 있다 할 수 있다.

〈표 3-26〉 개인정보 영향평가 심사 기준

분야	영역		상세내역	점검 항목수
계				122
대상기관의 개인정보보호 관리체계	1	개인정보 보호조직	개인정보 보호책임자 지정	2
			개인정보 취급자 지정	2
	2	개인정보 보호계획	개인정보 보호계획 수립	1
			개인정보 보호 교육계획 수립	1
	3	개인정보 처리방침	개인정보 처리방침 수립	7
	4	개인정보 파일관리	개인정보파일 관리·이용·제공 대장관리	5
			개인정보파일 파기사실관리	1
	5	개인정보 위탁 및 제공시 안전조치	개인정보 위탁시 안전조치	1
			개인정보 연계·제공시 안전조치	1
	6	개인정보 침해대응	침해사고 처리절차	4
	7	정보주체 권익보호	정보주체 권익보호	3
	8	개인정보 처리구역 보호	보호구역 지정	1
			개인정보 처리구역 통제	2
대상시스템의 개인정보 보호관리체계	1	대상시스템의 개인정보관리	개인정보 취급자 지정	1
			개인정보 취급자 의무	1
	2	개인정보 취급내용 공개	개인정보 파일의 안내	1
			개인정보 위탁관리 안내	1
			개인정보 제공 및 목적외 시용사실의 안내	3
			개인정보 파기사실의 안내	1
개인정보 처리단계별 보호	1	수집단계	개인정보 수집의 적합성	2
			개인정보 수집동의의 적합성	4
			개인정보 수집사실의 안내	2
			개인정보 수집시 보호조치	4
	2	저장 및 보유단계	개인정보파일 보유의 적합성 평가	2

분야	영역		상세내역	점검 항목수
			개인정보 파일대장의 작성	1
			개인정보 저장 및 보유시 암호화	1
	3	이용 및 연계·제공 단계	이용 및 제공의 기본원칙	3
			타기관 연계·제공시 절차	5
			개인정보처리시스템 접근통제	10
			웹 및 애플리케이션 통제	7
			개인정보 처리단말기 보호조치	5
			개인정보 이용·제공 승인	2
			네트워크 접속통제	4
			웹사이트 개인정보 노출차단	1
			개인정보 처리내역 기록관리	3
	4	파기단계	보유기간 산정 및 안내	3
특정 IT기술 활용시 개인정보보호	1	CCTV 활용	CCTV 설치시 의견수렴	1
			CCTV 설치 안내	1
			CCTV 사용제한	2
			CCTV 설치 및 관리에 대한 위탁	1
	2	RFID 활용	RFID 이용자 안내	4
			RFID 태그부착 및 제거	3
	3	바이오 정보활용	원본정보 보관시 보호조치	2
	4	위치정보 활용	개인위치정보 수집동의	1
			개인위치정보 제공시 안내사항	1

자료: 행정안전부·한국인터넷진흥원(2012), 개인정보영향평가수행안내서.

5. 일본의 프라이버시 마크(Privacy Mark, 일명 P 마크) 제도

일본은 우리나라의 주민번호와 같은 개인별 식별번호를 사용하고 있지는 않지만[19] 우리나라보다 앞서 2005년부터 개인정보의 보호에 관한 법률(이하 개인정보 보호법)이 시행되기 시작하였다.

19) 일본에서는 우리나라 '주민등록번호' 제도와 비슷한 일명 '마이넘버' 제도가 2016년부터 시행될 예정임.

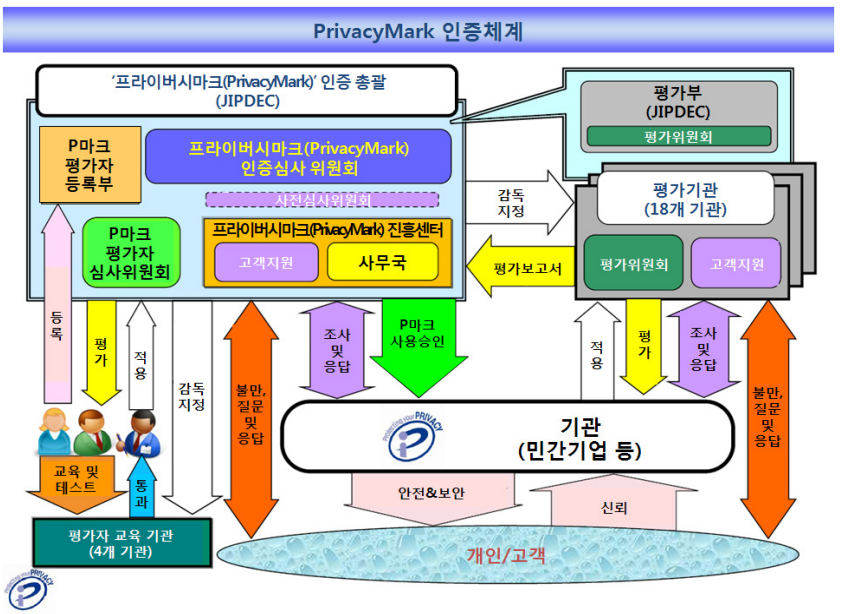
이러한 일본에서는 민간자율 규제적 성격의 인증제도인 프라이버시 마크, P 마크 제도를 통산성(通産省) 산하 공공기관인 일본정보처리개발센터(JIPDEC: Japan Information Processing Development Center)에서 주관하여 일찌감치 1998년부터 시행하고 있던 바, 2005년 4월 개인정보 보호법 전면시행을 계기로 P 마크 획득을 기본조건으로 제시하는 지방자치단체나 기업이 증가하면서(한국정보보호진흥원, 2009) 활성화가 이루어졌다.

본 제도는 개인정보 보호에 대한 소비자들의 인식을 향상시키고 소비자와 비즈니스 파트너들로부터 사회적 신뢰를 얻기 위한 기관들에게 인센티브 제공을 목적으로 하고 있으며 서면심사와 현장심사로 구성되어 있다. 인증기준은 서면 및 현장심사에서 총 210개 이상의 평가항목을 기준으로 PDCA개념(Plan-Do-Check-Act)에 기반을 두고 있다. P 마크 인증의 유효기간은 2년이며 심사기관으로 2013년 현재 지정된 민간사업자는 18개, 심사원 수 1,200여명, 그리고 이러한 심사원들을 교육하기 위한 심사원 교육기관도 4개가 운영되고 있다(JiPDEC, 2013, 그림 3-1 참조).

이러한 P 마크 인증체계는 농업, 임업, 어업, 광업, 건설업, 서비스업 등 총 13개 분야로 구분하여 시행되고 있으며 2013년 10월 15일현재 일본 내 P마크를 획득한 누적 기관 수는 13,252개, 그 중 가장 많은 분야는 서비스업으로 9,888개 기관이 획득하였다. 그 중에서도 의료기관은 의료업에 속하며 47개 기관이 획득한 것으로 나타나고 있다(표 3-27 참조).

일본의 P 마크 제도는 민간자율규제적인 특성을 반영하듯 정부의 정책적인 인센티브 제공보다는 자율적인 문화형성, 그리고 신뢰성 제고 효과를 꾀하고 있다(P마크제도 사이트 중 ‘P마크 부여사업자 일람’, [인용 2013.10.20.]).

〔그림 3-1〕 일본 P마크 인증체계 구성도



자료: JiPDEC(2013), The PrivacyMark System.

〈표 3-27〉 업종별 일본 P 마크 발급현황

분류	사업자 수
계	13,252
농업	1
임업	0
어업	0
광업	0
건설업	195
제조업	1,400
전기·가스·열공급·수도업	16
운수·통신업	564
도매·소매업, 음식점	795
금융·보험업	250
부동산	143

분류		사업자 수
서비스업	소계	9,888
	세탁·이발·목욕탕업	8
	주차사업	7
	기타 생활관련 서비스업	126
	여관, 기타숙소	5
	오락업	15
	자동차 정비업	5
	기계·가구등 수리업	34
	물품 임대업	32
	영화비디오 제 작업	62
	방송업	77
	정보서비스 조사업체	5,451
	광고업	522
	전문서비스업	626
	협동조합	22
	기타사업 서비스업	2,503
	폐기물 처리업	85
	의료업	47
	보건위생	129
	사회보험, 사회복지	53
	교육	30
	학술연구기관	8
	정치·경제·문화단체	41
공무		0

자료: P마크제도 사이트 중 'P마크 부여사업자 일람',
http://privacymark.jp/certification_info/list/clist.html, [인용 2013.10.20.].

일본은 개인정보 보호와 관련하여 총괄적인 통합방식과 더불어 분할방식을 동시에 취하고 있는 2중구조의 법률체계로(이자성, 2007) 분야별 가이드라인이 활발하게 제정·적용되고 있을 뿐 아니라 인증체계가 매우 안정화되어 있다. 이는 개인정보 보호의 중요성에 대한 사회적 인식이 일찌감치 자리하고 있고 이를 통해 자율적인 문화형성의 결과로 보여지어

우리나라에서 현재 실시 혹은 실시 예정하고 있는 인증제도 안정화를 위해 의미하는 바가 크다 할 수 있다.

6. 의료기관 인증제도

의료기관 인증제란 '의료법' 제58조(의료기관 인증)에 근거하여 환자의 안전과 의료서비스의 질 향상을 위해 2011년 1월부터 의료기관의 자율적인 참여를 취지로 시행하고 있는 제도로 '의료기관평가인증원'이 인증전담기관으로 수행하고 있다. 또한 동법 제58조의3(의료기관 인증기준 및 방법등) 제1항에 의하면 인증기준으로는 환자의 권리와 안전, 의료기관의 의료서비스 질 향상 활동, 의료서비스의 제공과정 및 성과, 의료기관의 조직·인력관리 및 운영, 환자만족도 등을 포함하며, 일정수준을 달성한 의료기관에 대해 유효기간 4년인 인증마크를 부여하게 된다(국가법령정보센터 사이트, [인용 2013.06.15.]).

인증대상은 모든 의료기관으로, 병원급 의료기관은 자율적으로 인증을 신청할 수 있으며 다만, 상급종합병원과 전문병원의 경우에는 지정기준에 해당되므로 인증조사를 받아야 한다. 한편 요양병원은 2013년부터 의무적으로 인증신청을 하도록 하고 있다. 인증기준은 기본가치체계, 환자진료체계, 행정관리체계, 성과관리체계 4개 측면으로 구성하여 의료기관의 규모 및 특성 즉, 대형병원, 중소병원, 요양병원, 정신병원에 따라 선택적 또는 단계적으로 적용하고 있다(의료기관평가인증원 사이트, [인용 2013.06.15.], 그림 3-2 참조).

〔그림 3-2〕 의료기관 인증기준체계

자료: 의료기관평가인증원 사이트, www.koiha.or.kr, [인용 2013.06.15.].

먼저 대형병원(300병상 이상)의 인증기준은 4개 측면, 13개 장, 42개 범주, 84개 기준에 의해 총 408개 조사항목으로 구성되어 있으며 이 중 개인정보와 관련된 내용은 환자권리존중 범주 중 환자 진료정보 보호에 대한 항목, 의료정보관리체계 범주 중 의료정보/의무기록 관리규정, 규정에 따른 의료정보/의무기록 접근제한 및 관리항목, 개인정보보호 및 보안 범주 중 개인정보보호 및 보안관련 규정, 개인정보보호를 위한 보안체계, 개인정보관리책임자 및 실무담당자 업무수행여부, 접근통제구역에 대한 출입 및 정보시스템 접근권한관리, 정보시스템 접속이력관리에 대한 항목등 총 8개 항목에 불과하였다(보건복지부·의료기관평가인증원, 2011a, 표 3-28 참조). 이중 개인정보보호 및 보안범주 내 5개항목은 500병상 이상의 대형병원에 시범적용하고 있다.

〈표 3-28〉 대형병원 인증기준 구성

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
Ⅰ. 기본가치 체계	1장. 안전보장활동	환자안전	
		직원안전	
		환경안전	
	2장. 지속적인 질 향상	질향상 운영체계	
		부서 질 향상 활동	
		환자 안전활동	
		지표 관리체계	
Ⅱ. 환자진료 체계	3장. 진료전달체계와 평가	진료전달체계	
		환자평가	
		검사체계	
	4장. 환자진료	환자진료체계	
		중증환자진료체계	
	5장. 수술 및 마취진정 관리	수술관리	
		마취진정관리	
	6장. 약물관리	약물관리체계	
		구매선정 및 보관	
		조제	
		투약 및 모니터링	
	7장. 환자권리존중 및 보호	환자권리존중	- 환자의 진료정보 보호 (의무기록 열람 금지)
		불만고충처리	
		동의서	
		장기이식관리	
Ⅲ. 행정관리 체계	8장. 경영 및 조직운영	조직운영(의료기관)	
		조직운영(임상진료)	
		조직운영(부서단위)	
		경영관리	
		의료윤리경영	
	9장. 인적자원관리	인적자원관리	
		직원교육	
		의료인력 충족성	
	10장. 감염관리	감염 관리체계	
		특수부서 감염관리	

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
	11장. 안전한 시설 및 환경관리	시설환경 안전관리체계	
		설비시스템	
		보안관리	
		위험물질관리	
		재난관리	
	12장. 의료정보관리	의료정보 관리체계	- 의료정보/의무기록 관리규정 - 규정에 따른 의료정보/의무기록 접근제한 및 관리
		의무기록 완결도 관리	
		의료정보수집 및 정보공유활동	
		개인정보보호 및 보안	- 개인정보보호 및 보안 관련규정 - 개인정보보호를 위한 보안체계 - 개인정보관리책임자 및 실무담당자 업무수행 - 접근통제구역에 대한 출입 및 정보시스템 접근권한관리 - 정보시스템 접속이력 관리
Ⅳ. 성과관리 체계	13장. 임상질 지표	임상질지표	

자료: 보건복지부·의료기관평가인증원(2011a), 2011 의료기관 인증조사 기준집(대형병원용).

중소병원(300병상 미만) 인증기준은 3개 측면, 12개 장, 36개 범주, 66개 기준에 의한 총 308개 조사항목으로 구성되어 있으며 이 중 개인정보와 관련된 내용은 환자권리존중 범주 중 환자 진료정보 보호에 대한 항목, 의료정보관리체계 범주 중 의료정보/의무기록 관리규정, 규정에 따른 의료정보/의무기록 접근제한 및 관리항목 등 3개 항목에 불과하다(보건복지부·의료기관평가인증원, 2011b, 표 3-29 참조).

〈표 3-29〉 중소병원 인증기준 구성

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
Ⅰ. 기본가치 체계	1장. 안전보장활동	환자안전	
		직원안전	
		환경안전	
	2장. 지속적인 질 향상	질향상 운영체계	
		부서 질 향상 활동	
		환자 안전활동	
		지표 관리체계	
Ⅱ. 환자진료 체계	3장. 진료전달체계와 평가	진료전달체계	
		환자평가	
		검사체계	
	4장. 환자진료	환자진료체계	
		중증환자진료체계	
	5장. 수술 및 마취진정 관리	수술관리	
		마취진정관리	
	6장. 약물관리	약물관리체계	
		구매선정 및 보관	
		조제	
		투약 및 모니터링	
	7장. 환자권리존중 및 보호	환자권리존중	- 환자의 진료정보 보호
		불만고충처리	
		동의서	
		장기이식관리	
Ⅲ. 행정관리 체계	8장, 경영 및 조직운영	조직운영(의료기관)	
		조직운영(임상진료)	
		경영관리	
		의료윤리경영	
	9장. 인적자원관리	인적자원관리	
		직원교육	
	10장. 감염관리	감염 관리체계	
		특수부서 감염관리	

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
	11장. 안전한 시설 및 환경관리	시설환경 안전관리체계	
		설비시스템	
		보안관리	
		위험물질관리	
	12장. 의료정보관리	의료정보 관리체계	- 의료정보/의무기록 관리규정 - 규정에 따른 의료정보/의무기록 접근제한 및 관리
		의무기록 완결도 관리	

자료: 보건복지부·의료기관평가인증원(2011b), 2011 의료기관 인증조사 기준집(중소병원용).

다음으로 요양병원 인증기준은 3개 측면, 11개 장, 27개 범주, 49개 기준에 의한 총 203개 조사항목으로 구성되어 있으며 이 중 개인정보와 관련된 내용은 환자권리존중 범주 중 환자의 진료정보 보호 항목과 의료정보 관리체계 범주 중 의료정보/의무기록 관리규정, 규정에 따른 의료정보/의무기록 접근제한 및 관리항목 등 3개 항목에 불과하다(보건복지부·의료기관평가인증원, 2012a, 표 3-30 참조).

〈표 3-30〉 요양병원 인증기준 구성

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
Ⅰ. 기본가치체계	1장. 안전보장활동	환자안전	
		직원안전	
		환경안전	
	2장. 지속적인 질 향상	질향상 운영체계	
		환자안전활동	
		의료서비스만족도	
Ⅱ. 환자진료체계	3장. 진료전달체계와 평가	진료전달체계	
		환자평가	
		검사체계	

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
	4장. 환자진료	환자진료체계	
		중증환자진료체계	
	5장. 약물관리	보관	
		조제	
		투약	
	6장. 환자권리존중 및 보호	환자권리존중	- 환자의 진료정보 보호
		불만고충처리	
		동의서	
Ⅲ. 진료지원 체계	7장, 경영 및 조직운영	조직운영	
		경영관리	
		의료윤리경영	
	8장. 인적자원관리	인적자원관리	
		직원교육	
	9장. 감염관리	기구관련 감염관리	
		부서 감염관리	
	10장. 안전한 시설 및 환경관리	시설환경 안전관리체계	
		시설환경 안전관리	
	11장. 의료정보관리	의료정보 관리체계	- 의료정보/의무기록 관리규정 - 규정에 따른 의료정보/의무기록 접근제한 및 관리

자료: 보건복지부·의료기관평가인증원(2012a), 2013 요양병원 인증조사 기준집.

마지막으로 정신병원 인증기준은 3개 측면, 12개 장, 28개 범주, 53개 기준에 의한 총 198개 조사항목으로 구성되어 있으며, 이 중 개인정보와 관련된 내용은 환자권리존중 및 보호 범주 중 환자의 진료정보 보호 항목과 의료정보 관리체계 범주 중 의료정보/의무기록 관리규정, 규정에 따른 의료정보/의무기록 접근제한 및 관리항목, 그리고 개인정보보호 및 보안 범주 중 개인정보보호 및 보안관련 규정, 개인정보보호를 위한 보안체계, 개인정보관리책임자 및 실무담당자 업무수행여부, 접근통제구역에

대한 출입 및 정보시스템 접근권한관리, 정보시스템 접속이력관리에 대항 항목 등 총 8개 항목에 불과하였다(보건복지부·의료기관평가인증원, 2012b, 표 3-31 참조). 이중 개인정보보호 및 보안범주 내 5개항목은 시범적용하고 있다.

〈표 3-31〉 정신병원 인증기준 구성

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
Ⅰ. 기본가치 체계	1장. 안전보장활동	환자안전	
		직원안전	
		환경안전	
	2장. 지속적인 질향상	질향상 운영체계	
Ⅱ. 환자진료 체계	3장. 진료전달체계와 평가	진료전달체계	
		환자평가	
		검사체계	
	4장. 환자진료	환자진료체계	
		중증환자진료체계	
	5장. 수술 및 마취관리	수술관리	
		마취관리	
	6장. 약물관리	약물선정 및 보관	
		조제	
		투약	
	7장. 환자권리 존중 및 보호	환자권리와 의무	- 환자의 진료정보 보호
		불만 및 고충처리	
		동의	
Ⅲ. 행정관리 체계	8장. 경영 및 조직운영	조직운영	
		경영관리	
	9장. 인적자원관리	인적자원관리	
		직원교육	
	10장. 감염위생관리	감염관리체계	
	11장. 안전한 시설 및 환경관리	시설환경 안전관리체계	
		설비시스템	
		위험물질 및 위해도구 관리	

체계(system)	장(chapter)	범주(category)	개인정보보호관련 항목
	12장. 의료정보관리	의료정보 관리체계	- 의료정보/의무기록관리규정 - 규정에 따른 의료정보/의무기록 접근제한 및 관리
		의무기록 관리	
		개인정보보호 및 보안	- 개인정보보호 및 보안 관련규정 - 개인정보보호를 위한 보안체계 - 개인정보관리책임자 및 실무담당자 업무수행 - 접근통제구역에 대한 출입 및 정보시스템 접근권한관리 - 정보시스템 접속이력 관리

자료: 보건복지부·의료기관평가인증원(2012b), 2013 정신병원 인증조사 기준집.

7. 소결 및 시사점

인증제도는 개인정보 보호를 위해 기관차원의 필수적이고도 충분한 조건들을 갖추었는 지를 평가함에 있어, 이러한 기준에 도달하기 위해 필요한 절차와 조건들을 스스로 학습하고 이행하는 과정에서 조직 구성원들의 의식과 행동양식이 개선되고, 궁극적으로는 조직의 개인정보 보호수준이 향상됨에 그 의의가 있다 할 수 있다. 이를 위해서는 인증에 대한 신뢰와 요구, 책임감이 사회 전반적으로 확산되어 활발하게 수용되어야 스스로 실천하는 자율규제적인 문화가 조성될 수 있으리라 생각된다.

개인정보 보호 관련하여 우리나라의 각종 인증제도와 함께 일본의 P마크제도, 우리나라의 의료기관 인증제도에 대해 분석해본 결과, 먼저 우리나라 인증제도는 정보보호 관리체계 인증(ISMS) 까지 그 범위를 넓혀

보면[20] 방송통신위원회, 안전행정부, 그리고 미래창조과학부에 이르기까지 관할부처 및 이에 따른 인증기관이 나뉘어져 있고(표 3-32 참조), 이들 각 인증제도의 세부 평가내용이 크게 다르지 않아 이를 준용하여야 하는 기관 입장에서는 비용에 대한 부담 뿐 아니라 그 실효성에 대한 우려도 표하고 있다[21].

〈표 3-32〉 개인정보 보호관련 자율적, 규제적 성격의 제도현황(2013년 10월 현재)

구분	홈페이지 인증		PIMS	PIPL	PIA
	ePRIVACY	i-Safe			
관련법	정보통신망법 및 개인정보 보호법		정보통신망법	개인정보 보호법	개인정보 보호법
관련고시	-		개인정보보호 관리체계 인증 등에 관한 고시	개인정보 보호수준 인증 등에 관한 고시	개인정보 영향평가에 관한 고시
시행시기	2000년	2002년	2010년	2013년	2005년 (법적의무화: 2011년)
의무사항 여부	자율	자율	권고	권고	의무 (특정기준의 공공기관)
대상	기업 및 기관 홈페이지		정보통신 사업자	공공 및 의료,금융영역 민간기관	공공 및 민간기관
주관기관	개인정보보호협회		방송통신 위원회	안전행정부	안전행정부
인증기관			한국 인터넷진흥원	한국 정보화진흥원	안전행정부장관으로부터 지정받은 기관
인증항목수	86개 항목	136개 항목	124개	65개	120개
유효기간	1년	1년	3년	3년	시스템변경시
유효 인증기관수	138기관	58기관	29기관	-	-

20) 정보보호 관리체계 인증(ISMS) 제도는 2002년부터 '정보보호 관리체계 인증 등에 관한 고시'(미래창조과학부고시 제2013-36호)에 따른 기준의 적합성을 인증하는 제도로, 유효기간은 3년이며 미래창조과학부 주관 하에 한국인터넷진흥원이 인증기관으로 업무를 수행하고 있음.

21) ZDNet Korea(2013.06.20.) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130620082009&type=det; 데이터넷(2013.10.07.), http://www.datanet.co.kr/news/articleView.html?idxno=68727.

또한, 부문별 영역별로 나뉘어져 있는 일본의 P 마크제도와는 달리 우리나라는 아직까지 영역별 특성을 반영한 인증제도가 정착되지 못하고 있다.

이처럼 스스로 실천하는 자율규제적인 특성 속에서 볼 때 우리나라의 개인정보 보호관련 인증제도는 아직까지는 당위성 측면에서, 필요성 측면에서 폭넓게 확산되지 못하고 있는 실정이며 특히 의료기관의 경우 인식측면에서, 환경측면에서 더 많은 준비가 필요하다고도 할 수 있다.

그러므로 정부차원의 인증제도간 중복 혹은 유사성에 대한 정리 뿐 아니라 의료기관과 같이 특정 영역의 특성을 잘 반영할 수 있는 부문별 영역별 인증체계로의 정립이 매우 필요한 시점이라 할 수 있다.

한편 이와 같은 개인정보 보호관련 인증제도와 더불어 의료서비스의 질 향상을 위한 의료기관 인증제도에 있어 개인정보 보호측면을 보다 강화할 필요가 있다. 이에 현재 적용 혹은 시범운영 중인 개인정보 보호관련 인증기준 항목에 대해 정보의 생명주기(생성, 수집, 이용, 보관, 파기 등)에 따라, PDCA(Plan-Do-Check-Act) 모델에 따라 보다 구체화, 상세화, 그리고 보다 확대할 필요가 있다.

제4장 국내 의료기관의 개인정보보호 관리현황 및 개인의료정보보호에 대한 인식현황

제1절 조사설계

제2절 조사실시 및 조사결과

4 국내 의료기관의 개인정보보호 관리현황 및 개인의료정보보호에 대한 인식현황

제4장에서는 의원급 개인(의료)정보보호 관리현황과 의사의 인식현황, 병원급 개인(의료)정보보호 관리현황, 의료기관 홈페이지 개인정보처리방침 관리현황, 일반국민의 개인(의료)정보보호 인식현황을 파악하기 위한 조사설계, 조사실시, 그리고 이에 대한 조사결과를 정리하였다.

제1절 조사설계

1. 의원급 개인(의료)정보보호 관리현황 및 의사의 인식현황

의원급 의료기관의 개인(의료)정보보호 관리현황과 아울러 개원의 의사들의 개인(의료)정보보호에 대한 인식조사는 의원 원장을 대상으로 하였다. 의원은 구조상 개인의료정보보호를 위한 전담직원을 배치하기 어렵고 원장의 경우 해당기관 운영의 직접적인 책임이 있는 자 이므로 원장을 대상으로 개인정보보호 관리현황과 이에 대한 인식을 파악하는 것이 필요하다고 판단하였다.

조사 설문문항은 제3장에서의 관련 현황조사 분석결과를 토대로 하여 관련법률 및 고시등 분석, 공무원/관련 협단체/학계의 관계자 정책간담회의 등에서의 의견수렴을 통해 최종 문항을 선정하였다. 이렇게 선정된 설문문항은 응답자 및 의료기관 특성, 개인(의료)정보보호에 대한 인지정도, 개인(의료)정보보호 관리현황 등 크게 3개 부문으로 구분하였으며 먼저 응답자 및 의료기관 특성으로는 개원의 의사의 성별, 연령, 의원운영

기간, 주 진료과목, 지역, 정보시스템 관리·운영현황, 홈페이지 운영 및 관리·운영현황 등 8개 문항으로 구성하였다. 다음으로 개인(의료)정보보호에 대한 인지정도에서는 개인정보 보호법 내용에 대한 인지정도, 개인정보 보호법과 관련하여 정보를 얻는 곳, 개인정보 관련하여 정보주체의 권리에 대한 인지 정도, 개인정보 수집·이용에 대한 정보주체의 동의사항 내용 등 모두 15개 문항으로 구성하였다. 마지막으로 개인(의료)정보보호 관리현황에서는 개인정보 처리방침을 공개하는지, 개인정보처리시스템 각 항목에 대해 수행하고 있는지, 보안프로그램을 설치하고 운영하는지, 개인정보 파일 암호화를 위한 소프트웨어를 사용하는지, 개인정보보호 책임자의 역할이 무엇인지 등 17개 문항으로 구성하여 총 40개 항목으로 구성하였다(표 4-1 참조).

〈표 4-1〉 의원급 의료기관의 개인(의료)정보보호 관리현황 및 개원의 의사의 개인(의료)정보보호에 대한 인식조사 내용

구분	문항수	내용	관련 법 조항
응답자 및 의료기관 특성	8	성별, 만 연령, 개설 운영기간, 주 진료과목, 지역, 정보시스템 관리·운영 현황, 홈페이지 운영여부, 홈페이지 관리·운영 현황	
개인(의료)정보보호에 대한 인지도	15	개인정보 보호법 내용에 대한 인지정도	
		개인정보 보호법과 관련하여 정보를 얻는 곳(1~3순위)	
		개인정보 관련 정보주체의 권리에 대한 인지정도	개인정보 보호법 제4조 (정보주체의 권리)
		개인정보 수집·이용에 대한 정보주체의 동의사항	개인정보 보호법 제15조 (개인정보의 수집·이용), 제18조(개인정보의 이용·제공 제한), 제22조(동의를 받는 방법)
		정보주체의 동의가 필요한 경우 고지사항	개인정보 보호법 제15조 (개인정보의 수집·이용)
		개인정보보호와 관련된 교육을 받아본	

구분	문항수	내용	관련 법 조항
		경험여부	
		교육을 받아본 경험에 대한 효과 및 이행여부	
		교육을 받지 않은 이유	
		개인정보보호를 위해 필요한 교육내용	
		원장님이 생각하는 일반국민의 개인정보보호(의무기록)에 대한 관심수준(5점 척도)	
		개인정보보호와 관련된 염려 정도(5점 척도)	
		개인정보보호 중요도(5점 척도)	
		개인정보보호의 관리수준 정도(5점 척도)	
		개인정보보호 수준향상을 위한 인식제고 대상의 중요도(5점 척도)	
		개인정보보호 수준 향상을 위한 국가차원의 지원방법 중요도(5점 척도)	
개인(의료)정보보호	17	개인정보 처리방침 공개 여부	개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
		개인정보 처리방침 개별 항목에 대한 공개여부	
		개인정보처리시스템 각 항목에 대한 수행여부	개인정보의 안전성 확보조치기준 고시 제4조(접근권한의 관리), 제8조(접속기록의 보관 및 위·변조 방지)
		보안프로그램 설치 및 운영 여부	개인정보의 안전성 확보조치기준 고시 제9조(보안프로그램 설치 및 운영)
		비밀번호 관리에 대한 작성규칙 수립 및 이행여부	개인정보의 안전성 확보조치기준 고시 제5조(비밀번호 관리)
		개인정보처리시스템 각 항목별 암호화	개인정보의 안전성 확보조치기준 고시 제7조(개인정보의 암호화)
		개인정보 파일 암호화를 위한 소프트웨어 사용여부	
		개인정보처리구역에 대한 출입 통제 및 이력관리 여부	개인정보의 안전성 확보조치기준 고시 제10조(물리적 접근방지)
		개인정보가 기록된 문서 및 보조저장매체에 대한 관리여부	
		업무위탁 시 위탁자의 문서화필요사항	개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한), 동법 시행령 제28조(개인정보의 처
		업무위탁 시 위탁자가 수행하여야 할 사항	

구분	문항수	내용	관련 법 조항
			리업무 위탁시 조치)
		개인정보 처리단계별 과태료 부과항목	개인정보 보호법 제75조 (과태료)
		개인정보 유출 시 정보주체에게 알려야 할 내용	개인정보 보호법 제34조 (개인정보 유출 통지 등)
		영상정보처리기기의 관리 방안	개인정보 보호법 제25조 (영상정보처리기기의 설치·운영 제한)
		개인정보보호책임자 역할	개인정보 보호법 제31조(개인정보 보호책임자의 지정)
		기술적·관리적 보호조치 기준 의무규정	개인정보 보호법 제29조 (안전조치의무), 동법 시행령 제30조(개인정보의 안전성 확보조치)
		개인정보보호 관련 업무수행의 어려운 점 혹은 정부에 바라는 점	

한편 응답자의 접근성, 편의성, 용이성 등을 고려하여 본 연구원에서 사용 중인 'SPSS Survey PRO'를 활용하여 개발한 온라인 설문조사를 기본으로 하되, 일부 현장배포를 통한 서면 설문조사를 병행하기로 하였으며 설문조사는 전국 시·도 의사회 정보통신위원회의 협조 하에 진행키로 하였다.

2. 병원급 개인(의료)정보보호 관리현황

병원급 개인(의료)정보보호 관리현황을 파악하기 위한 조사는 병원의 개인정보보호 담당자를 대상으로 하였다.

조사 설문문항은 의원급과 마찬가지로 제3장에서의 관련 현황조사 분석결과를 토대로 관련법률 및 고시등 분석, 공무원/관련 협단체/학계의 관계자 정책간담회의 등에서의 의견수렴을 통해 최종 문항을 선정하였

다. 이렇게 선정된 설문문항은 병원의 일반적 특성, 관리체계 구축, 보호대책 수립 및 시행, 침해사고 대책, 개인정보 처리, 안전성 확보조치, 개인정보보호 업무수행 등 7개 영역으로 구분하여 구성하였다. 먼저 병원의 일반적 특성을 파악하기 위하여 의료기관의 형태와 특성, 지역, 정보시스템 관리·운영 현황, 홈페이지 개설 및 관리·운영 현황 등 5개 문항으로 구성하였으며 관리체계 구축현황을 파악하기 위해 개인정보보호 업무담당부서, 2013년도 개인정보보호 관련 예산 책정 여부, 개인정보보호 책임자의 지정 여부 및 역할 수행 여부, 업무위탁시 위탁자의 문서화 필요사항 및 위탁자가 수행하여야 할 사항, 2013년도 개인정보보호 교육계획 수립 여부, 대상자별 교육계획 수립여부 등 8개 문항으로 구성하였다.

개인정보보호대책 수립 및 시행영역에서는 개인정보 목적외 혹은 제3자제공 여부와 정보주체의 동의여부, 개인정보 처리방침 공개 여부 및 각 항목에 대한 공개여부, 영상정보처리기기 설치·운영 여부, 영상정보처리기기 관리방안 수행여부 등 6개 항목으로 구성하였으며 침해사고 대책영역에서는 개인정보 노출방지를 위한 안전조치의무 수행여부등 2개항목, 개인정보처리영역에서는 홈페이지 회원가입시 수집항목여부 등 2개 항목으로 구성하였다.

안전성 확보조치영역에서는 접근권한 및 접속기록에 대한 관리여부, 개인정보의 암호화 여부, 개인정보가 기록된 문서 및 보조저장매체에 대한 관리여부 등 8개 문항, 마지막으로 개인정보보호 업무수행 영역에서는 우리나라 의료기관 개인정보보호 관리수준에 대한 인지정도, 의료기관 개인정보보호 수준향상을 위한 인식제고 대상의 중요도, 의료기관 개인정보보호 수준향상을 위한 국가차원의 지원방법별 중요도 등 9개 문항으로 구성하여 병원을 대상으로 한 조사표는 총 40개 항목으로 구성하였다(표 4-2 참조).

〈표 4-2〉 병원급 의료기관의 개인정보보호 관리현황 조사내용

구분	문항수	내용	관련 법 조항
일반적 특성	5	의료기관의 형태와 특성, 지역, 정보시스템 관리·운영현황, 홈페이지 운영여부, 홈페이지 관리·운영 현황	
관리체계 구축	8	개인정보보호 업무 담당부서	
		'13년도 개인정보보호 관련 예산여부	개인정보 안전성확보조치 고시 제3조(내부관리계획의 수립·시행)
		개인정보보호책임자의 지정 여부	개인정보보호법 제31조(개인정보 보호책임자의 지정)
		개인정보보호책임자의 역할 수행 여부	
		업무위탁 시 위탁자의 문서화 필요사항	개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리제한), 동법 시행령 제28조(개인정보의 처리업무 위탁시 조치)
		업무위탁 시 위탁자 수행사항	
		'13년도 개인정보보호 교육계획 수립여부	개인정보 보호법 제31조(개인정보 보호책임자의 지정), 제28조(개인정보취급자에 대한 감독)
		개인정보보호 교육 대상자별 교육계획 수립여부	
보호대책 수립 및 시행	6	개인정보 목적 외 혹은 제3자제공여부	개인정보 보호법 제18조(개인정보의 이용·제공 제한), 제17조(개인정보의 제공)
		개인정보 목적 외 혹은 제3자 제공 시 정보주체의 동의 여부	
		개인정보 처리방침 공개 여부	개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
		개인정보 처리방침 개별 항목에 대한 공개 여부	
		영상정보처리기기의 설치·운영 여부	개인정보보호법 제25조(영상정보처리기기의 설치·운영 제한)
		영상정보처리기기 관리방안 수행여부	
침해사고 대책	2	개인정보 노출방지를 위한 안전조치의무 수행 여부	개인정보 보호법 제29조(안전조치의무), 동법 시행령 제30조(개인정보의 안전성 확보조치), 개인정보의 안전성 확보조치 기준고시 제9조(보안프로그램 설치 및 운영)
		개인정보 유·노출 및 침해사고 발생에 대한 대응절차 유무	개인정보 보호법 제34조(개인정보 유출 통지등, 동법 시행령 제40조(개인정보 유출 통지의 방법 및 절차)
개인정보 처리	2	홈페이지 회원가입 시 수집항목 여부	
		홈페이지 회원가입 시 본인확인 수단	

구분	문항수	내용	관련 법 조항
안전성 확보조치	8	개인정보처리시스템 각 항목에 대한 수행여부	개인정보의 안전성 확보조치 기준 고시 제4조(접근권한의 관리), 제8조(접속기록의 보관 및 위·변조 방지)
		보안프로그램 설치 및 운영 여부	개인정보의 안전성 확보조치 기준 고시 제9조(보안프로그램 설치 및 운영)
		개인정보처리시스템 각 항목별 암호화	개인정보의 안전성 확보조치 기준 고시 제7조(개인정보의 암호화)
		개인정보 파일 암호화를 위한 소프트웨어 사용여부	
		개인정보를 보조저장매체로 전달할 경우 암호화 여부	
		비밀번호 관리에 대한 작성규칙 수립 및 이행여부	개인정보의 안전성 확보조치 기준 고시 제5조(비밀번호 관리)
		개인정보처리구역에 대한 출입 통제 및 이력관리 여부	개인정보의 안전성 확보조치 기준 고시 제10조(물리적 접근 방지)
		개인정보가 기록된 문서 및 보조저장매체에 대한 관리여부	
개인정보 보호 업무수행	9	우리나라 의료기관 개인정보보호 관리수준에 대한 인지 정도(5점 척도)	
		본 원의 개인정보보호 관리수준 정도(5점 척도)	
		의료기관 개인정보보호 수준향상을 위한 인식제고 대상의 중요도(5점 척도)	
		의료기관 개인정보보호 수준 향상을 위한 국가차원의 지원방법 중요도(5점 척도)	
		개인정보 유출 시 정보주체에게 알려야 할 내용	개인정보 보호법 제34조(개인정보의 유출 통지 등)
		영상정보처리기기의 관리 방안	개인정보보호법 제25조(영상정보처리기기의 설치·운영 제한)
		개인정보보호책임자의 관리·감독 역할	개인정보 보호법 제31조(개인정보 보호책임자의 지정)
		기술적·관리적 보호조치 기준의 의무규정 인지정도	개인정보보호법 제29조(안전조치의무), 동법 시행령 제30조(개인정보의 안전성 확보 조치)
		의료기관 개인정보보호 관리수준향상을 위한 업무수행의 어려운 점 혹은 정부에 바라는 점	

한편 응답자의 접근성, 편의성, 용이성 등을 고려하여 본 연구원에서 사용 중인 'SPSS Survey PRO' 를 활용하여 개발한 온라인 설문조사를 기본으로 하되, 일부 현장배포를 통한 오프라인 설문조사를 병행하기로 하였으며 설문조사는 대한병원협회, 대한중소병원협의회, 대한병원정보협회, 전국지방의료원연합회 등의 협조를 통해 수행하기로 하였다.

3. 의료기관 홈페이지 개인정보처리방침 관리현황

개인정보 처리방침은 개인정보를 처리하는 기준 및 보호조치로써, 개인정보 보호법 제30조에서 이를 수립 및 공개토록 규정하고 있다. 또한 동법 시행령 제31조에서는 이에 대한 내용 및 공개방법을, 표준 개인정보 보호지침 제34조에서 제38조까지에서는 개인정보 처리방침의 공개, 변경, 작성기준, 필수적 기재사항, 임의적 기재사항을 제시하고 있다.

이에 홈페이지 개인정보처리방침 관리현황은 건강보험심사평가원에 등록·공개되어 있는 의료기관 중 상급종합병원, 종합병원, 병원, 의원 등 총 30,000여개 의료기관을 대상으로 하였다. 먼저 이들 의료기관들의 홈페이지 유무를 상용검색포털에서 검색한 후, 홈페이지가 있는 경우 개인정보 처리방침의 게재여부, 게재되어 있다면 필수적으로 공개하게 되어 있는 처리목적, 처리및보유기간, 제3자제공 사항, 위탁사항, 권리 및 의무사항, 처리항목, 파기사항, 보호책임자 사항, 방침변경사항, 안전성 확보조치 사항 등 10개항목 각각이 게시되어 있는지, 그리고 게시되어 있는 각 항목이 제대로 충분하게 기술되어 있는지에 대한 조사문항을 구성하였다(표 4-3 참조).

〈표 4-3〉 의료기관 홈페이지 개인정보처리방침 조사항목

구분	조사항목
처리목적	홈페이지 회원관리, 건강정보제공, 병원홍보, 결제서비스 등과 같이 개인정보 처리목적이 구체적으로 기재되어 있는가?
처리 및 보유기간	정보주체로부터 동의받은 '보유·이용기간' 혹은 법령에 의한 '보유·이용기간'이 기재되어 있는가?
제3자 제공사항	정보주체의 동의를 받거나 법률의 규정 등 개인정보 보호법이 허용한 경우 이외에는 개인정보를 제3자에게 제공하지 않는다는 원칙이 기재되어 있는가?
위탁 사항	개인정보 처리업무 위탁시 위탁받는 자, 위탁하는 업무 내용 등이 개재되어 있는가?
권리, 의무사항	정보주체가 지니는 개인정보 열람, 정정·삭제, 처리정지 등 행사방법, 행사절차 등을 구체적으로 기재했는가?
처리항목	처리하고 있는 개인정보 각 항목을 기재하고 있는가?
파기사항	개인정보 불필요시 지체없이 파기한다는 내용 및 방법이 개재되어 있는가?
보호책임자 사항	개인정보보호를 총괄해서 책임지는 개인정보 보호책임자의 성명, 직책, 연락처가 제대로 기재되어 있는가?
방침변경 사항	개인정보 처리방침의 시행일자, 그간의 변경이력이 기재되어 있는가?
안전성 확보조치 사항	내부관리계획 수립·시행, 개인정보에 대한 접근통제 및 접근권한의 제한 조치, 암호화기술 적용, 접속기록 보관 및 위변조 방지 조치, 보안프로그램 설치 및 갱신 등 관리적/기술적/물리적 조치사항을 기재하고 있는가?

해당의료기관 홈페이지 분석은 연구진의 지도 하에 4명의 대학재학생이 조사문항 및 관련 법 조항에 대한 충분한 숙지 후 수행하기로 하였다.

4. 일반국민의 개인(의료)정보보호 인식현황

일반국민 대상의 개인(의료)정보보호에 대한 인식 조사는 제3장에서의 관련 현황조사 분석결과와 Smith et al.(1996)에 의해 이미 개발되고 그 타당성이 검증된 바 있는 조직의 정보 프라이버시 정책에 대한 개인의 관심정도를 측정하고 확인하는 도구 등을 참고로 하여 공무원/관련 협단체/학계의 관계자 정책간담회의 등에서의 의견수렴을 통해 최종 설문문항

을 도출하였다.

조사문항은 응답자 특성, 의료기관 이용특성, 개인의료정보보호에 대한 관심정도, 개인정보보호에 대한 인식 등 크게 4개 영역으로 구분하여 먼저 응답자 특성 영역에서는 응답자의 성별, 만 연령, 결혼상태, 최종학력, 직업, 월평균 가구소득, 거주지역 등 7개 문항으로 구성하였으며 의료기관 이용특성으로는 최근 1년간 주로 이용한 의료기관 유형 및 의료기관 방문횟수 2개 문항으로 구성하였다. 다음으로 개인의료정보보호에 대한 관심에서는 개인정보의 수집, 정확성, 접근성, 불법 등으로 상세구분하여 질문지를 구성하였으며 마지막으로 개인정보보호에 대한 인식에서는 개인정보 보호법 내용에 대한 인지정도, 개인정보에 대한 정보주체의 권리 인지정도, 항목별 개인정보보호 중요도에 대한 인지정도 등 5개 항목으로 구성하여 총 15개 항목으로 구성하였다(표 4-4 참조).

〈표 4-4〉 개인건강정보 보호에 대한 일반국민 인식조사 내용

구분	문항수	내용	관련 법 조항
응답자 특성	7	성별, 만 연령, 결혼상태, 최종학력, 직업, 월평균 가구소득, 거주지역	
의료기관 이용특성	2	최근 1년간 주로 이용한 의료기관 유형	
		최근 1년간 의료기관 방문 횟수	
개인의료정보 보호에 대한 관심	1	수집(Collection), 실수(Error) or 정확성(accurate), 접근(Access), 불법(Unauthor)에 대한 관심정도(5점 척도)	
개인정보보호에 대한 인식	5	개인정보 보호법 내용에 대한 인지정도	
		개인정보에 대한 정보주체의 권리 인지정도	개인정보 보호법 제4조(정보주체의 권리)
		항목별 개인정보보호 중요도에 대한 인지정도(5점 척도)	
		항목별 개인정보보호 관리수준에 대한 인지정도(5점 척도)	
		개인건강정보보호를 위한 바램	

일반국민 대상의 조사는 건강관련 포털(건강정보광장, 금연길라잡이, 건강길라잡이)과 본 연구원 홈페이지의 협조를 받아 진행하기로 하였다.

이상과 같은 4개영역에 대한 설문조사 내용, 조사대상, 조사방법, 조사항목, 협조기관 등에 대해 정리해보면 〈표 4-5〉와 같다.

〈표 4-5〉 본 연구에서의 의료기관 개인(의료)정보보호 관리현황 및 인식현황 파악을 위한 조사 개요

조사내용	조사대상	조사방법	조사항목	협조기관
의원급 개인의료정보 보호 관리현황 및 의사 인식현황	의료인 (의원 원장)	온라인조사/ 오프라인조사	3개부문 총 40개 항목	전국 시도의사회 정보통신위원회
병원급 개인의료정보 보호 관리현황	병원 (개인정보보호 담당자)	"	7개부문 총 40개 항목	대한병원협회, 대한중소병원협의회, 대한병원정보협회, 전국지방의료원연합회
의료기관 홈페이지 개인정보 처리방침 관리현황	심평원등록 의료기관 홈페이지 (상급종합병원, 종합병원, 병원, 의원)	홈페이지 분석	개인정보 처리방침 10개항목	-
일반국민 개인의료정보 보호 인식현황	일반국민	온라인조사	4개부문 총 15개 항목	건강길라잡이, 금연길라잡이, 건강정보광장등 건강포털 및 보사연 홈페이지

제2절 조사실시 및 조사결과

1. 의원급 개인(의료)정보보호 관리현황 및 의사의 인식현황

본 조사는 16개 시·도 의사회 정보통신위원회 임원진 및 소속의원 원장의

사들을 대상으로 2013년 9월 23일 ~ 2013년 10월 25일까지 약 1달가량 온라인 설문조사와 더불어 오프라인 서면 설문조사 형태로 실시하였으며, 응답은 총 105명이 참여하였다.

수집된 자료는 SPSS 21 통계프로그램을 활용하여 통계처리 하였으며, 변수에 관한 빈도분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하였다.

가. 응답자 및 의료기관 특성

분석대상 총 응답자 수는 105명으로 남성 92.4%, 여성 7.6% 분포를 보이고 있었으며, 연령대로는 40세미만(6.7%), 40대(40.4%), 50대(43.3%), 60세이상(9.6%) 순으로 나타났다. 의원 운영기간은 10년이상이 전체 중 67.0%를 차지하였으며 주 진료과목으로는 내과(20.0%), 가정의학과(11.4%), 정형외과(10.5%) 순으로 나타났다. 또한 개설하여 운영하고 있는 지역으로는 비수도권(76.2%)이 수도권보다 월등히 높게 나타났다(표 4-6 참조).

정보화현황[22]에서는 응답 의원 중 25.0%가 홈페이지를 개설하여 운영 중이었으며 이에 대한 운영은 자체관리 26.9%, 위탁관리 53.8%, 자체와 위탁을 병행하여 관리 19.2%로 나타났다(표 4-7 참조).

의원급 대상 조사의 응답자 및 의료기관 특성에 대한 분석결과 눈여겨 볼 사항은 홈페이지 운영에 있어 외부에 위탁관리하는 경우가 많다는 것이다. 이는 앞에서도 언급하였듯이 그만큼 환자의 개인의료정보에 대해 외부인력들의 접근성이 높다는 것으로써, 이는 의료기관입장에서는 외부

22) 정보화 현황 중 OCS(입원, 외래), EMR(입원, 외래) 도입현황에 대한 조사문항은 OCS, EMR에 대해 의료기관별, 응답자별 기준이 명확하지 않아 분석결과에 대한 정확성이 떨어진다는 일부 응답자의 의견에 따라 본 분석결과에 포함하지 않기로 하였음.

위탁에 대한 철저한 관리와 더불어 외부 위탁업체 입장에서도 이에 대한 자체교육 및 인식제고가 필요하다 하겠다.

〈표 4-6〉 의원급 조사응답자의 일반적 특성

(단위: 명, %)

구분		응답자수	%
성	계	105	100.0
	남자	97	92.4
	여자	8	7.6
연령대	계	104	100.0
	40세 미만	7	6.7
	40~49세	42	40.4
	50~59세	45	43.3
	60세 이상	10	9.6
의원 운영기간	계	103	100.0
	5년 미만	11	10.7
	5~10년 미만	23	22.3
	10~15년 미만	25	24.3
	15~20년 미만	23	22.3
	20년 이상~	21	20.4
주 진료과목	계	105	100.0
	내과	21	20.0
	정신건강의학과	4	3.8
	가정의학과	12	11.4
	외과	7	6.7
	정형외과	11	10.5
	신경외과	4	3.8
	산부인과	4	3.8
	소아청소년과	8	7.6
	안과	6	5.7
	이비인후과	9	8.6
	피부과	8	7.6
	비뇨기과	5	4.8
	영상의학과	2	1.9
	재활의학과	3	2.9
	마취통증의학과	1	1.0
지역	계	105	100.0
	수도권	25	23.8
	비수도권	80	76.2

〈표 4-7〉 의원급 조사응답기관의 정보화 현황

(단위: 명, %)

구분		응답자수	%
홈페이지 개설	계	104	100.0
	예	26	25.0
	아니오	78	75.0
홈페이지 관리·운영	계	26	100.0
	자체관리	7	26.9
	위탁관리	14	53.8
	자체+위탁 병행관리	5	19.2

나. 개인의료정보 보호 인지도

개인정보 보호법에 대해 의원 원장선생님들이 어느정도 알고 있는지를 물어본 결과, 대충 알고 있는 경우가 42.9%로 가장 많았으며 어느정도 혹은 잘 알고 있는 경우는 32.4%로 나타났다(표 4-8 참조).

〈표 4-8〉 개인정보 보호법에 대한 의원급 의사들의 인지도 현황

(단위: 명, %)

구분	응답자수	%
계	105	100.0
전혀 들어본 적 없다	1	1.0
들어는 보았으나, 잘 알지 못한다	25	23.8
대충 알고 있으나 다른사람에게 설명할 수준은 아니다	45	42.9
알고 있으며, 다른사람에게 간략히 설명할 수 있는 수준이다	26	24.8
정확하게 알고 있으며, 다른 사람에게 상세히 설명할 수 있는 수준이다	8	7.6

이들이 개인정보 보호법 관련하여 가장 많이 정보를 얻는 곳으로 1순위는 관련 협·단체, 2순위는 의료계 동료, 3순위는 인터넷 검색이 각각 1위를 나타내었으며 1, 2, 3순위를 모두 더했을 경우에는 의료계 동료, 관련 협·단체, 그리고 인터넷 검색 순으로 나타났다. 이는 향후 관련자료 배포 및 교육 시행에 있어 많은 고려요인이 될 것이다(표 4-9 참조).

〈표 4-9〉 의원급 의사들의 개인정보 보호법 관련한 정보취득처

(단위: %)

구분	계	1순위	2순위	3순의
계	100.0	100.0	100.0	100.0
대중매체(TV, 신문) 홍보	17.5	18.1	11.4	23.1
(의료계) 동료	25.1	18.1	39.0	18.3
인터넷 검색	19.5	18.1	10.5	29.8
관련 협·단체 제공자료	23.5	39.0	21.0	10.6
관련 교육 및 세미나 참석	8.0	3.8	10.5	9.6
시스템 관련업체	6.4	2.9	7.6	8.7

다음으로 개인정보 보호법 관련하여 정보주체가 누릴 수 있는 권리, 즉 개인정보 처리에 관한 정보를 제공받을 권리, 개인정보 처리에 관한 동의 여부 및 범위를 선택할 권리, 개인정보 처리여부 확인 및 열람을 요구할 수 있는 권리, 개인정보 처리에 대한 정지·정정·삭제·파기를 요구할 수 있는 권리, 신속하고 공정한 절차에 따라 구제받을 권리 등 5개 권리에 대해 알고 있는지 물어본 결과, 5개 권리에 대해 평균 65.1%가 알고 있었으며 그 중 개인정보 처리여부 확인 및 열람을 요구할 권리에 대해 가장 많이 알고(75.2%) 있는 것으로 나타났다. 한편 구제받을 권리와 처리 정지·정정·삭제·파기요구에 대한 권리가 각각 53.3%로 상대적으로 낮게 나타났다(표 4-10 참조).

〈표 4-10〉 개인정보보호 관련 권리에 대한 의원급 의사들의 인지도 현황

(단위: 명, %)

구분	계		알고 있음		모르고 있음	
	응답자수	%	응답자수	%	응답자수	%
평균				65.1		34.9
개인정보 처리정보 제공받을 권리	105	100.0	77	73.3	28	26.7
개인정보 처리 동의여부 및 범위 선택 권리	105	100.0	74	70.5	31	29.5
개인정보 처리여부 확인 및 열람 요구 권리	105	100.0	79	75.2	26	24.8
개인정보 처리 정지·정정·삭제·파기 요구 권리	105	100.0	56	53.3	49	46.7
신속하고 공정한 절차에 따라 구제받을 권리	105	100.0	56	53.3	49	46.7

다음은 개인정보 수집·이용에 대한 정보주체(법정대리인 포함)의 동의사항에 대해 제대로 알고 있는지를 확인한 결과, 정답률은 평균 80.9%를 나타냈다. 각 항목별로는 만 14세 미만 아동에 대한 개인정보 수집시 법정대리인의 동의가 필요한 것과, 홈페이지 회원가입 및 각종 게시판에서 개인정보 수집시 정보주체의 동의가 필요한 것은 각각 99.0%, 96.2%로 거의 대부분 알고 있는 것으로 나타난 반면 오히려 진료목적으로 개인정보 수집시 정보주체에게 별도로 동의없이 가능한 사실에 대해서는 60.0%만이 알고 있는 것으로 나타났다(표 4-11 참조). 사실상 진료목적이라 하더라도 정보주체의 동의를 받는 것은 개인정보 보호에 해를 끼치거나 법에 위배되는 것은 아니나, 진료목적의 경우 의료법에 우선하여 개인정보 보호법에서 요구하는 동의를 받지 않아도 되는 바, 이는 개인정보보호법에 대한 정확한 이해도 부족이라는 것을 나타내는 단면이라고도 볼 수 있다.

〈표 4-11〉 개인정보 수집·이용에 대한 정보주체의 동의사항에 대한 의원급 의사들의 인지도 현황

(단위: 명, %)

구분	계		정답		오답	
	응답자수	%	응답자수	%	응답자수	%
평균				80.9		19.1
진료목적의 개인정보 수집시 정보주체 별도 동의없이 가능	105	100.0	63	60.0	42	40.0
진료목적 이외 개인정보 수집시 별도 동의없이 가능	105	100.0	79	75.2	26	24.8
법률에 규정되어 있거나 법령상 의무준수를 위한 경우 별도 동의없이 가능	105	100.0	78	74.3	27	25.7
홈페이지 회원가입 및 각종 게시판에서 개인정보 수집시 동의 필요	105	100.0	101	96.2	4	3.8
만14세 미만 아동에 대해 개인정보 수집시 법정대리인 동의 필요	105	100.0	104	99.0	1	1.0

또한 정보주체의 동의 필요시 고지해야할 사항에 대해 제대로 알고 있는지를 확인한 결과, 정답률은 평균 96.4%를 나타내 사실상 고지사항에 대해서는 대다수가 알고 있는 것으로 나타났다(표 4-12 참조).

〈표 4-12〉 개인정보 수집·이용에 있어 고지필요사항에 대한 의원급 의사들의 인지도 현황

(단위: 명, %)

구분	계		정답		오답	
	응답자수	%	응답자수	%	응답자수	%
평균				96.4		3.6
개인정보의 수집·이용 목적	105	100.0	102	97.1	3	2.9
수집하려는 개인정보 항목	105	100.0	103	98.1	2	1.9
개인정보 보유 및 이용기간	105	100.0	99	94.3	6	5.7
동의거부 권리에 대한 사실 및 동의 거부에 따른 불이익 발생시 이에 대한 사실	105	100.0	101	96.2	4	3.8

개인정보 보호관련 교육에 있어서는 최근 1년동안 응답자의 8.6%만이 교육을 받은 경험이 있다고 답하였으며, 교육을 받지 않은 이유로는 충분한 정보 및 소개가 부족하여 45.8%, 시간을 내지 못하여, 필요성을 못 느껴, 적절한 교육내용을 찾지 못하여 순으로 나타났다(표 4-13 참조).

〈표 4-13〉 개인정보보호관련 교육경험 여부 및 미경험 사유

(단위: 명, %)

구분		응답자수	%
교육경험 여부	계	105	100.0
	예	9	8.6
	아니오	96	91.4
미경험사유	계	96	100.0
	필요성을 못 느껴서	18	18.8
	시간을 내지 못하여	19	19.8
	충분한 정보 및 소개 부족으로	44	45.8
	적절한 교육내용을 찾지 못하여	15	15.6

또한 개인정보 보호를 위해 필요한 교육내용에 대한 주관식 질문에서는 법적인 규제내용, 반드시 지켜야 할 법조항 등을 답하였으며 교육방식에 있어서도 실 업무에 맞추어 사례중심을 원한다고 하였다.

이러한 결과로 볼 때, 의원급 의사들을 대상으로는 의료현장에서 반드시 지켜야 할 사항들에 대한 맞춤형 교육자료에 의한 교육과 더불어 교육에 대한 홍보, 개인의료정보 보호의 중요성에 대한 홍보가 필요하리라 판단된다.

의원 원장선생님들이 생각하는 우리나라 일반국민이 의료기관에서 관리 중인 본인의 개인정보(의무기록등)보호에 대한 관심수준에서는, 5점 만점에 평균 2.21점으로 보통보다 낮다고 생각하고 있었으며, 반면 의사

들은 진료실에서 수집된 환자의 개인정보 유출 우려에 대해 평균 3.19점의 염려정도를, 그리고 의원에서의 개인정보보호 관리수준에 대한 내원환자의 항의가 우려된다에 대해서는 평균 3.11점의 보통보다 약간 높은 염려정도를 나타냈다. 이로 볼 때, 의사들은 개인의료정보에 대해 일반국민들의 관심정도는 낮다고 생각하는 반면, 본인 진료실에서의 개인정보 유출에는 그다지 많은 우려를 보이지 않고 있는 것으로 생각할 수 있다(표 4-14 참조).

〈표 4-14〉 의사가 생각하는 일반국민의 관심정도 및 진료환경에서의 우려정도

구분	관심 및 우려정도
일반국민이 본인 개인정보(의무기록등)에 대한 관심수준	2.21
진료실에서 수집된 환자의 개인정보 유출에 대한 우려	3.19
의원에서의 개인정보보호 관리수준에 대한 내원환자의 항의 우려	3.11

개인정보를 일반적인 개인정보(이름, 주민등록번호, 전화번호등), 의료기관 이용에 의해 생성·관리되는 개인의무기록정보, 국민건강보험공단 등 공공기관에 의해 생성·관리되는 개인건강관리정보(건강검진정보 등), 건강포털 이용에 의해 생성·관리되는 개인건강관리정보, 건강관련 모바일 앱 이용에 의해 생성·관리되는 개인건강관리정보 등으로 나누었을 때 각각에 대해 의사들이 생각하는 개인정보보호 중요도를 조사한 결과, 5점 만점에 평균 4.06점으로 나타났다. 그 중에서 개인의무기록정보는 4.28점, 그리고 공공기관에서의 개인건강관리정보, 일반개인정보, 건강포털 및 모바일 앱에 의한 개인건강관리정보 순으로 나타나 의사들은 의료기관에서 생성, 관리되는 개인의무기록정보가 제일 중요하다고 생각하는 것으로 나타났다(표 4-15 참조).

〈표 4-15〉 항목별 개인정보보호 중요도에 대한 의사들의 인지도 현황

구분	중요도
평균	4.06
일반개인정보	4.04
개인의무기록정보	4.28
공공기관에 의한 개인건강관리정보	4.22
건강포털에 의한 개인건강관리정보	3.90
모바일 앱에 의한 개인건강관리정보	3.90

또한 일반적인 개인정보보호, 병원급 의료기관에서의 개인의무기록정보 보호, 의원급에서의 개인의무기록정보 보호, 공공기관에서의 개인건강관리정보 보호, 건강포털에서의 개인건강관리정보 보호, 건강관련 모바일 앱에서의 개인건강관리정보 보호, 응답자의 해당 의원에서의 개인의무기록정보 보호 관리수준에 대해 물어본 결과 5점 만점에 전체 평균은 2.94점으로 중요도(평균 4.06점)에 비하면 관리수준이 낮다고 생각하였다. 그 중에서는 본인 의원에서의 개인 의무기록정보 보호 관리수준에 대해 가장 높게 그리고 병원, 의원, 일반개인정보, 공공기관, 건강포털, 모바일 앱 순으로 평가하고 있었다(표 4-16 참조). 이는 상대적으로 의료기관에서의 개인정보 보호수준을 높게 평가하고는 있으나 앞에서 인지하고 있는 중요도에 비해서는 전체적으로 관리수준이 낮다고 생각하는 것을 알 수 있다.

다음으로 의료기관 개인정보보호 수준향상을 위한 CEO(의료기관 최고 결정권자), 의료기관 직원, 개발업체 직원, 소비자(환자) 각 대상의 인식제고 중요도에서는 5점 만점에 평균 3.89점으로 나타났으며 CEO, 의료기관직원, 개발업체 직원이 각각 3.96점, 3.94점, 3.93점 순으로 나타

나 이들간 중요도에 있어서는 큰 차이를 보이지 않고 있다(표 4-17 참조). 이는 곧 의료기관 개인정보 보호 수준향상을 위해서는 CEO, 의료기관 직원, 개발업체 직원에 있어 차별없는 인식제고가 필요한 것으로 판단한 것으로 생각할 수 있다.

〈표 4-16〉 항목별 개인정보보호 관리수준에 대한 의사들의 인지도 현황

구분	개인정보보호 관리수준
평균	2.94
일반개인정보 보호	2.97
병원에서의 개인의무기록정보 보호	3.33
의원에서의 개인의무기록정보 보호	3.15
공공기관에서의 개인건강관리정보 보호	2.83
건강포털에서의 개인건강관리정보 보호	2.48
모바일 앱에서의 개인건강관리정보 보호	2.46
본인 의원에서의 개인 의무기록정보 보호	3.38

〈표 4-17〉 의사들이 생각하는 대상별 인식제고에 대한 중요도

구분	중요도
평균	3.89
CEO(의료기관 최고 결정권자)	3.96
의료기관 직원	3.94
개발업체 직원	3.93
소비자(환자)	3.73

의사들이 생각하는 국가차원의 지원방법 종류별 중요도는 5점 만점에 평균 3.82점을 나타내었으며 그 중에서 기술적 지원과 가이드라인 배포에 대해 상대적으로 중요도를 높게 생각하고 있었다(표 4-18 참조).

〈표 4-18〉 의사들이 생각하는 국가차원의 지원방법별 중요도

구분	중요도
평균	3.82
기술적 지원(솔루션 도입등)	3.92
국가차원의 적극적 홍보	3.85
개인정보보호 관련교육	3.77
의료기관용 가이드라인 배포	3.92
개선방안을 위한 자문 지원(컨설팅 등)	3.62

다. 개인의료정보보호 관리현황

개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)에 의하면, 개인정보 처리방침에 대해 홈페이지 혹은 사업장 공개여부와 더불어 10가지 필수항목에 대해 고지하게 되어 있다. 이에 따라 조사한 결과, 개인정보 처리방침은 46.7%가 공개하고 있다고 답하였으며 필수 10개 항목 각각에 대해서는 처리목적(83.7%)과 처리항목(81.6%)을 가장 많이 포함하고 있었고 상대적으로 파기사항(57.1%)과 처리방침 변경사항(59.2%)에 대한 포함정도는 낮게 나타났다(표 4-19 참조).

이상과 같은 결과를 보았을 때, 개인정보 처리방침에 대한 수립 및 이에 대한 공개에 대한 정확한 인지가 부족하다고 생각할 수 있으며 10개 필수 공개항목에 대해서도 명확한 인지가 부족하다고 생각할 수 있다.

〈표 4-19〉 의원급 조사응답기관의 개인정보 처리방침 공개여부 및 포함항목 현황

(단위: 명, %)

구분		응답자수	%
공개여부	계	105	100.0
	예	49	46.7
	아니오	44	41.9
	모르겠음	12	11.4
포함항목	처리목적		83.7
	처리 및 보유기간		75.5
	제3자 제공		69.4
	처리 위탁		61.2
	정보주체의 권리·의무 및 행사방법		73.5
	처리 항목		81.6
	파기사항		57.1
	보호책임자 사항		69.4
	처리방침 변경 사항		59.2
	안전성 확보조치 사항		65.3

다음으로 개인정보의 안전성 확보조치 기준 고시 제4조(접근권한의 관리) 및 제8조(접속기록의 보관 및 위·변조 방지)에 의해 필요한 항목 즉, 개인정보처리시스템에 대해 접근권한을 업무수행에 필요한 최소한 범위로 차등부여하는지, 인사이동 발생시 접근권한 변경 또는 말소를 수행하고 있는지, 접근권한에 대한 내역을 기록하고 최소 3년간 보관하고 있는지, 개인정보취급자의 접속기록을 생성하는지, 개인정보취급자의 접속기록을 6개월이상 보관 및 관리하고 있는지, 개인정보취급자의 접속기록을 점검 및 후속조치하고 있는지 등을 조사하였다. 분석결과 평균 20.5%로 매우 낮게 나타났으며 그 중에서도 취급자 접속기록 생성과 접속기록 점

검 및 후속조치는 15.2%로 수행정도가 가장 낮게 나타났다(표 4-20 참조). 또한 각 항목에 대해 모른다고 응답한 경우도 모두 30%가 넘게 나타난 바, 이는 사실상 의원을 실제 운영하고 있는 원장들의 경우 기술적 내용에 대한 이해가 용이하지 않기 때문인 것으로 판단된다.

〈표 4-20〉 의원급 조사응답기관의 개인정보처리시스템에 대한 항목별 수행현황

(단위: 명, %)

구분	계		예		아니오		모르겠음	
	응답자수	%	응답자수	%	응답자수	%	응답자수	%
평균				20.5		43.8		35.7
업무권한 차등부여	105	100.0	33	31.4	39	37.1	33	31.4
인사이동에 따른 접근권한 변경 또는 말소	105	100.0	25	23.8	44	41.9	36	34.3
접근권한 내역기록 및 최소 3년간 보관	105	100.0	22	21.0	46	43.8	37	35.2
취급자 접속기록 생성	105	100.0	16	15.2	49	46.7	40	38.1
취급자 접속기록 6개월 이상 보관 및 관리	105	100.0	17	16.2	49	46.7	39	37.1
접속기록 점검 및 후속조치	105	100.0	16	15.2	49	46.7	40	38.1

다음으로 해당의원에 대한 보안조치 상황에 대한 결과에서는 보안프로그램 설치 및 정기적인 업데이트를 수행하고 있는지, 비밀번호 작성규칙을 수립하여 이를 준수하고 있는지, 개인정보처리시스템에 저장하는 고유식별정보 등을 암호화하고 있는지, 업무PC내 개인정보 포함 화일을 암호화하기 위한 소프트웨어를 사용하고 있는지, 개인정보처리구역(전산실, 자료보관실 등)에 대해 비인가자의 출입을 통제하고 출입에 따른 이력을 관리하고 있는지, 개인정보 기록문서 및 보조저장매체를 금고 또는 시건장치가 있는 캐비넷등 안전한 장소에 보관하고 있는지 등에 대해 설

문조사를 실시하였다. 조사결과 평균 32.1% 이행정도를 나타내었으며 그 중 보안프로그램 설치 및 정기적인 업데이트가 82.9%로 가장 많이 이행하고 있었으나 상대적으로 암호화, 개인정보처리구역에 대한 출입통제와 출입이력관리에 대한 이행률은 전반적으로 낮게 나타났다(표 4-21 참조). 이 역시 모른다고 응답한 경우도 항목에 따라서는 30%가 넘게 나타나 보안조치사항에 대해 원장들의 관심이 더 필요할 것으로 판단된다.

〈표 4-21〉 의원급 조사응답기관의 보안조치 현황

(단위: 명, %)

구분		계		예		아니오		모르겠음	
		응답자수	%	응답자수	%	응답자수	%	응답자수	%
평균					32.1		43.1		24.8
보안프로그램 설치 및 정기적인 업데이트		105	100.0	87	82.9	13	12.4	5	4.8
비밀번호 작성규칙 수립 및 준수		105	100.0	57	54.3	34	32.4	14	13.3
암호화	고유식별정보	104	100.0	20	19.2	46	44.2	38	36.5
	바이오정보	105	100.0	11	10.5	51	48.6	43	41.0
	비밀번호	105	100.0	26	24.8	40	38.1	39	37.1
개인정보 암호화를 위한 소프트웨어 사용		105	100.0	12	11.4	56	53.3	37	35.2
개인정보처리구역에 대한 출입통제 및 출입이력관리		105	100.0	18	17.1	67	63.8	20	19.0
개인정보 기록물에 대한 안전한 보관		105	100.0	39	37.1	55	52.4	11	10.5

개인정보관리 규정에 대한 인지현황에서는 외부에 개인정보 업무위탁 시 문서화 필요사항 및 수행업무 내용, 개인정보 보호법 위반 시 과태료부과 사항, 개인정보 유출시 정보주체에게 수행하여야 하는 고지사항, 영상정보처리기기 관리방안, 개인정보처리에 관한 관리·감독 역할, 기술적·관리적 보호조치 기준 의무규정사항 등을 제대로 알고 있는지 조사하였다.

조사결과, 문서화에 대해서는 정답률이 평균 45.2%, 모르겠다고 응답한 경우도 43.5%로 나타나 정확히 알고 있는 경우는 그리 높지 않은 것으로 생각된다. 또한 외부에 개인정보처리 업무 의뢰시 위탁자가 수행하여야 하는 업무를 잘 아는 지 파악하기 위해 관련항목들에 대한 인지여부를 조사하였는 바, 위탁 개인정보처리업무 내용 공개, 위탁받는 수탁자 정보 공개, 재화 또는 서비스 홍보 및 판매권유 업무 위탁시 업무내용과 수탁자를 정보주체에게 통지, 수탁자가 개인정보 분석·유출·변조·훼손하지 않도록 교육, 수탁자가 개인정보 안전처리에 대한 감독, 수탁자의 개인정보 보호 준수여부 정기점검 등 각 항목이 수행하여야 하는 사항인지를 물어본 결과, 정답률은 평균 50.8%, 모르겠다고 응답한 경우 45.7%로 나타났다. 그 외 유출시 정보주체에게 알려야 하는 사항, 기술적·관리적 보호조치기준 의무규정에 대해서는 정답률이 각각 78.8%, 78.8%로 상대적으로 높게 나타났다(표 4-22 참조). 결과적으로 개인정보관리 규정 중 특히 외부로 업무위탁시 준수해야 할 사항에 대한 인식제고를 위한 노력이 필요하리라 생각된다.

마지막으로 의료기관 개인정보보호 관리에 있어 일선에서의 어려운 점 혹은 정부에 바라는 점에 대한 주관식 문항에서는 개인정보 보호법 적용에 있어 일관적인 적용보다는 의료현장에 맞는 보다 완화된 규제 적용, 주민번호 대체방안 강구, 체계적인 교육, 상세한 가이드라인 제공, 인력지원과 예산투자 등 순으로 의견을 제시하였다.

〈표 4-22〉 의원급 조사응답기관의 개인정보관리 규정 인지현황

(단위: 명, %)

구분		계		정답		오답		모르겠음	
		응답자수	%	응답자수	%	응답자수	%	응답자수	%
문서화	평균				45.2		11.3		43.5
	위탁업무 수행목적외 개인정보처리금지사항	103	100.0	46	44.7	15	14.6	42	40.8
	개인정보 기술적, 관리적 보호조치사항	103	100.0	48	46.6	13	12.6	42	40.8
	업무위탁 목적 및 범위	103	100.0	48	46.6	11	10.7	44	42.7
	재위탁 제한 사항	103	100.0	48	46.6	11	10.7	44	42.7
	개인정보에 대한 안전성확보조치사항	103	100.0	49	47.6	10	9.7	44	42.7
	위탁업무관련 개인정보 관리현황 점검등 감독사항	103	100.0	47	45.6	11	10.7	45	43.7
	수탁자 준수의무 위반시 손해배상 사항	103	100.0	46	44.7	12	11.7	45	43.7
외부업무의뢰시 위탁자 수행업무	평균				50.8		3.5		45.7
	위탁 개인정보처리업무 내용공개	103	100.0	54	52.4	5	4.9	44	42.7
	수탁자 정보공개	103	100.0	54	52.4	5	4.9	44	42.7
	홍보 혹은 판매권유업무 위탁시 업무내용,수탁자 정보주체에게 통지	103	100.0	50	48.5	3	2.9	50	48.5
	개인정보 분실, 유출, 변조, 훼손하지 않도록 교육	103	100.0	56	54.4	2	1.9	45	43.7
	수탁자의 개인정보처리 감독	103	100.0	55	53.4	3	2.9	45	43.7
	수탁자의 개인정보보호 준수여부 정기점검	103	100.0	51	49.5	4	3.9	48	46.6
과태료 부과항목		95	100.0	62	65.3	33	34.7	-	-
유출시 정보주체에게 알려야할 내용		99	100.0	78	78.8	21	21.2	-	-
영상정보처리기기 관리방안		99	100.0	75	75.8	24	24.2	-	-
개인정보보호책임자의 관리·감독 역할		99	100.0	50	50.5	49	49.5	-	-
기술적·관리적 보호조치기준 의무규정		99	100.0	78	78.8	21	21.2		

2. 병원급 개인(의료)정보보호 관리현황

병원을 대상으로 한 조사는 9월 27일부터 10월 25일까지 약 1달간 온라인 설문조사와 더불어 오프라인 서면 설문조사를 병행하여 실시하였으며, 응답은 총 105개 병원이 참여하였다.

수집된 자료는 SPSS 21 통계프로그램을 활용하여 통계처리 하였으며 변수에 관한 빈도분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하였다.

가. 일반적 특성

분석대상 응답 병원수는 총 105개소로 상급종합병원 10개소(9.5%), 종합병원 53개소(50.5%), 병원 42개소(40.0%) 이었으며, 이중 교육병원은 41개소(39.0%)로 나타났다. 이들의 개설지역은 수도권이 31.4%, 비수도권이 68.6%를 나타내고 있었으며 공공(지방공사의료원)은 24.8%, 민간은 75.2%를 차지하고 있었다(표 4-23 참조).

조사응답병원의 평균 병상규모는 약 345병상이었으며 병상규모별 분포는 〈표 4-24〉와 같다.

정보화현황[23]에서는 병원 대부분(92.4%) 홈페이지를 개설.운영하고 있었으며 홈페이지는 위탁관리(39.2%)와 자체 및 위탁을 병행한 관리(39.2%)가 동일하게 나타났다(표 4-25 참조). 병원급 의료기관에서도 홈페이지 운영에 있어 외부에 위탁관리하는 경우가 많다는 것은 외부인력들의 정보접근성이 높다는 것으로 외부위탁에 대한 철저한 관리가 필요하다 하겠다.

---

23) 정보화 현황 중 OCS(입원, 외래), EMR(입원, 외래) 도입현황에 대한 조사문항은 OCS, EMR에 대해 의료기관별, 응답자별 기준이 명확하지 않아 분석결과에 대한 정확성이 떨어진다는 일부 응답자의 의견에 따라 본 분석결과에 포함하지 않기로 하였음.

〈표 4-23〉 병원급 조사응답기관의 특성

(단위: 개소, %)

구분		응답 병원 수	%
종류	계	105	100.0
	상급종합병원	10	9.5
	종합병원	53	50.5
	병원	42	40.0
지역	계	105	100.0
	수도권	33	31.4
	비수도권	72	68.6
공공/민간	계	105	100.0
	공공의료기관	26	24.8
	민간의료기관	79	75.2

〈표 4-24〉 병원급 조사응답기관의 병상규모

(단위: 개소, %)

구분	응답 병원 수	%
계	105	100.0
~ 99병상	13	12.4
100 ~ 199병상	27	25.7
200 ~ 299병상	21	20.0
300 ~ 399병상	11	10.5
400 ~ 499병상	10	9.5
500병상 이상	23	21.9

〈표 4-25〉 병원급 조사응답기관의 정보화현황

(단위: 개소, %)

구분		응답 병원 수	%
홈페이지 개설	계	105	100.0
	예	97	92.4
	아니오	8	7.6
홈페이지 관리·운영	계	97	100.0
	자체관리	21	21.8
	위탁관리	38	39.2
	자체+위탁 병행관리	38	39.2

나. 관리체계 구축

2013년도 개인정보보호 예산책정 현황에서는 개인정보보호 교육·홍보 예산(자문비, 교통비, 운영비, 결과보고서 등 포함), 개인정보 관리·감독/컨설팅/모니터링 예산, 보안시스템(F/W, IDS, IPS, UTM등) 도입·운영 예산, 백신 SW 도입·운영예산 등 4개 영역에 대한 예산책정 현황을 조사한 결과, 보안시스템(71.4%)과 백신 SW(81.0%) 도입·운영예산에 비해 교육·홍보 혹은 관리·감독/컨설팅/모니터링을 위한 예산책정 비율이 낮게 나타났다(표 4-26 참조). 이는 개인정보보호 관련 예산 책정에 있어 각 의료기관들이 개인정보처리자의 인식제고, 행태변화 등을 위한 컨설팅, 모니터링, 교육, 홍보는 단기간에 효과를 보이기 어렵고 보안시스템이라던가 백신 SW 도입 등은 바로 효과가 나타나기 때문인 것으로 생각할 수도 있고, 한편으로는 관련 HW, SW보다는 컨설팅, 모니터링, 교육, 홍보 등에 대한 다양한 접근이 어렵기 때문인 것으로도 생각할 수 있다.

〈표 4-26〉 응답병원의 개인정보보호 예산책정 현황

(단위: 개소, %)

구분	계	공공/민간		유형		
		공공병원	민간병원	상급병원	종합병원	병원
전체	105(100.0)	26(24.8)	79(75.2)	10(9.5)	53(50.5)	42(40.0)
개인정보보호 교육·홍보 예산	31(29.5)	4(15.4)	27(34.2)	6(60.0)	14(26.4)	11(26.2)
개인정보관리·감독, 컨설팅,모니터링 예산	25(23.8)	3(11.5)	22(27.8)	4(40.0)	11(20.8)	10(23.8)
보안시스템 도입·운영 예산	75(71.4)	21(80.8)	54(68.4)	10(100.0)	38(71.7)	27(64.3)
백신 SW 도입·운영 예산	85(81.0)	26(100.0)	59(74.7)	10(100.0)	45(84.9)	30(71.4)

한편 예산현황에 있어 공공과 민간에 따라, 병원 유형별로 차이를 나타내고 있었는데 공공과 민간을 비교해보았을 때 교육·홍보와 컨설팅·모니

터링 예산은 공공병원보다는 상대적으로 민간병원의 예산책정 비율이 높았으며 보안시스템 도입 및 백신SW 도입 등과 같은 인프라 측면에 있어서는 공공병원의 예산책정 비율이 더 높게 나타났다. 이는 어쩌면 민간병원보다 공공병원이 인프라 구축을 위한 예산확보가 용이하기 때문일 것으로 판단해볼 수 있다. 또한 병원 유형별로 보았을 때, 모든 항목에서 상급병원의 예산책정비율이 상대적으로 높게 나타났다.

병원에서 개인정보보호 업무담당인력(전임 혹은 겸임)은 평균 1.7명으로, 그 중 1명이 54.5%로 가장 많았으며 2명(26.3%), 3명(11.1%), 4명(4.0%), 5명 이상(4.0%) 순으로 나타났다.

한편 병원급의 88.6%는 책임자가 지정되어 있었는데 이를 공공/민간별, 병원유형별로 살펴보면 공공병원과 민간병원은 별 차이가 없었으며 병원유형별로는 상급종합병원의 경우는 100%, 그리고 종합병원, 병원 순으로 나타났다(표 4-27 참조).

〈표 4-27〉 응답병원의 개인정보보호 책임자 지정 현황

(단위: 개소, %)

구분		전체병원 수	책임자 지정병원 수
계		105	93(88.6)
공공/민간	공공병원	26	23(88.5)
	민간병원	79	70(88.6)
병원유형	상급종합병원	10	10(100.0)
	종합병원	53	48(90.6)
	병원	42	35(83.3)

각 병원의 개인정보 보호책임자의 수행업무 현황에 대해서는 개인정보보호계획 수립 및 시행, 개인정보 처리실태 및 관행의 정기적인 조사 및 개선, 개인정보 처리관련 불만처리와 피해구제, 개인정보 유출 및 오남용 방지를 위한 내부통제시스템 구축 등 모두 4가지 항목에 대해 조사하였다.

분석결과 공공 vs. 민간병원 비교에서는 계획 수립 및 시행정도는 공공병원, 민간병원 모두 약 81.0%로 나타나 비교적 많은 기관에서 수행하고 있었으나 나머지 3개 항목에 대해서는 공공병원보다 민간병원에서 수행정도가 높았고 민간병원의 경우에도 65~70% 정도로 그다지 높지는 않게 나타났다. 병원유형별 결과에서는 다른 문항 결과와는 다르게 4개 항목 모두 종합병원보다 병원의 수행정도가 오히려 높게 나타났다(표 4-28 참조).

〈표 4-28〉 응답병원의 공공/민간병원별, 유형별 개인정보 보호책임자 수행업무 현황

(단위: 개소, %)

구분	계	공공/민간		유형		
		공공병원	민간병원	상급병원	종합병원	병원
전체	93(100.0)	23(24.7)	70(75.3)	10(10.8)	48(51.6)	35(37.6)
개인정보 보호 계획 수립 및 시행	85(91.4)	21(80.8)	64(81.0)	10(100.0)	43(89.6)	32(91.4)
개인정보 처리실태 등에 대한 정기적인 조사 및 개선	63(67.7)	12(46.2)	51(64.6)	8(80.0)	28(58.3)	27(77.1)
개인정보 처리관련 불만처리 및 피해구제	70(75.3)	15(57.8)	55(69.6)	9(90.0)	31(64.6)	30(85.7)
개인정보 유출, 오남용방지를 위한 내부통제시스템 구축	65(69.9)	12(46.2)	53(67.1)	9(90.0)	31(64.6)	25(71.4)

다음으로 개인정보 업무위탁시 문서화가 필요한 내용 즉 수행목적외 개인정보 처리금지에 관한사항, 개인정보의 기술적/관리적 보호조치 사항, 업무위탁 목적 및 범위, 재위탁 제한 내용, 개인정보 안전성 확보조치 내용, 위탁업무 관련 감독에 관한 내용, 수탁자 의무위반시 손해배상등에 관한 내용 등에 대해 물어본 결과, 정답률은 평균 86.3%로 나타났다. 또한 업무위탁 시 위탁자(병원)가 수행하여야 하는 업무를 잘 아는 지 파악하기 위해 관련항목들에 대한 인지여부를 조사하였다. 위탁 개인정보처

리업무 내용 공개, 위탁받는 수탁자 정보공개, 재화 또는 서비스 홍보 및 판매권유 업무 위탁시 업무내용과 수탁자를 정보주체에게 통지, 수탁자가 개인정보 분석·유출·변조·훼손하지 않도록 교육, 수탁자가 개인정보 안전처리에 대한 감독, 수탁자의 개인정보보호 준수여부 정기점검 등 각 항목이 수행하여야 하는 사항인지를 물어본 결과, 정답률은 평균 81.9% 로 나타나 전체적으로 인지정도가 많이 떨어지지는 않았다(표 4-29 참조).

〈표 4-29〉 병원급 조사응답기관의 개인정보관리 규정 인지현황

(단위: 개소, %)

구분		계		정답		오답		모르겠음	
		병원수	%	병원수	%	병원수	%	병원수	%
문서화	평균				86.3		4.4		9.4
	위탁업무 수행목적외 개인정보처리금지사항	105	100.0	96	91.4	1	1.0	8	7.6
	개인정보 기술적, 관리적 보호조치사항	105	100.0	96	91.4	2	1.9	7	6.7
	업무위탁 목적 및 범위	105	100.0	91	86.7	6	5.7	8	7.6
	재위탁 제한 사항	105	100.0	80	76.2	13	12.4	12	11.4
	개인정보에 대한 안전성확보조치사항	105	100.0	93	88.6	3	2.9	9	8.6
	위탁업무관련 개인정보 관리현황점검등 감동사항	105	100.0	88	83.8	5	4.8	12	11.4
	수탁자 준수의무 위반시 손해배상 사항	105	100.0	90	85.7	2	1.9	13	12.4
외부업무의뢰시 위탁자 수행업무	평균				81.9		6.2		11.9
	위탁 개인정보처리업무 내용공개	105	100.0	84	80.0	9	8.6	12	11.4
	수탁자 정보공개	105	100.0	83	79.0	11	10.5	11	10.5
	홍보 혹은 판매권유업무 위탁시 업무내용,수탁자 정보주체에게 통지	105	100.0	81	77.1	9	8.6	15	14.3
	개인정보 분실, 유출, 변조, 훼손하지 않도록 교육	105	100.0	89	84.8	4	3.8	12	11.4
	수탁자의 개인정보처리 감독	105	100.0	89	84.8	4	3.8	12	11.4
	수탁자의 개인정보보호 준수여부 정기점검	105	100.0	90	85.7	2	1.9	13	12.4

2013년도 개인정보보호 교육계획은 전체기관 중 61개소(58.1%) 만이 수립되어 있었으며 '아니오'라고 응답한 44개소(41.9)를 제외하고, 교육계획 수립 대상자를 조사한 결과, 개인정보취급자, 책임자, 일반직원 중에서는 일반직원이 95.1%로 가장 높게 나타났다(표 4-30 참조).

〈표 4-30〉 병원급 조사응답기관의 개인정보보호 교육계획 수립여부

(단위: 개소, %)

구분		응답 병원 수	%
개인정보보호 교육계획 수립여부	계	105	100.0
	예	61	58.1
	아니오	44	41.9
개인정보 취급자	예	54	88.5
	아니오	7	11.5
개인정보보호 책임자	예	49	80.3
	아니오	12	19.7
일반직원	예	58	95.1
	아니오	3	4.9

다. 보호대책 수립 및 시행

개인정보 목적 외 이용 혹은 제3자 제공 시 91.3%가 정보주체의 동의를 받고 있었으며, 개인정보처리방침에 대해 81.0%가 공개하고 있다고 답하였다. 필수 10개 항목 각각에 대해서는 처리목적(89.5%)과 처리 및 보유기간(82.6%), 정보주체의 권리·의무 및 행사방법(82.6%)을 가장 많이 포함하고 있었으며 상대적으로 처리위탁(57.0%), 제3자제공(58.1%)에 대한 포함정도는 낮게 나타났다(표 4-31 참조).

〈표 4-31〉 병원급 조사응답기관의 개인정보 처리방침 공개여부 및 포함항목 현황

(단위: 개소, %)

구분		응답 병원 수	%
공개여부	계	105	100.0
	예	85	81.0
	아니오	14	13.3
	모르겠음	6	5.7
포함항목	처리목적		89.5
	처리 및 보유기간		82.6
	제3자 제공		58.1
	처리 위탁		57.0
	정보주체의 권리·의무 및 행사방법		82.6
	처리 항목		81.4
	파기사항		76.7
	보호책임자 사항		80.2
	처리방침 변경 사항		75.6
	안전성 확보조치 사항		70.9

영상정보처리기기 설치 및 운영 관련하여 전체 병원 중 90.5%가 설치·운영하고 있었으며 이 때 필요항목별 수행정도는 안내판설치 93.7%, 안전성 확보조치 80.9%, 녹음기능 사용 금지조치 74.5%, 관리대장 68.1% 순의 수행정도를 나타냈다.

라. 침해사고 대책

침해사고 대책에서는 개인정보 노출방지, 침해사고 대응절차에 관한 분석결과로 개인정보 노출방지를 위한 수행정도에서는 백신소프트웨어

설치·운영 95.2%, F/W, IDS, IPS, UTM 등과 같은 보안시스템 설치·운영 74.3%, 개인정보 등록금지 등과 같은 홈페이지 게시판 공지 73.3%, 개인정보 암호화 Tool 설치·운영 61.0%, 가상사설망(VPN) 설치·운영 58.1%, 홈페이지 노출점검 Tool 설치·운영 36.2% 순의 이행정도를 나타내었으며 개인정보 침해사고 대응절차는 응답병원 중 62.5%가 확립하고 있는 것으로 나타났다.

마. 개인정보 처리

홈페이지 회원가입시 수집하는 항목은 이름(83.7%), 전화번호(76.9%), 이메일주소(72.1%), 주소(65.4%), 주민등록번호(33.7%) 순이었으며 사용하고 있는 인증수단으로는 주민등록번호(32.7%), 아이핀(26.0%), 휴대폰인증(17.3%), 공인인증(12.5%), 신용카드인증(4.8%) 순으로 나타나(표 4-32 참조) 아직까지 홈페이지 회원가입 시 주민등록번호를 본인인증을 위해 많이 사용하는 것으로 확인되었다. 그러나 이는 개정된 개인정보 보호법이 2014년 시행되기 전에 이에 대한 조치방안이 강구되어야 할 것으로 생각된다.

바. 안전성 확보조치

안전성 확보조치 수행을 위한 개인정보처리시스템에서의 항목별 수행정도에서는 6개항목에 대한 평균 59.5%, 그 중 인사이동에 따른 접근권한 변경 또는 말소조치는 84.8%로 가장 높게, 접속기록 점검 및 후속조치는 40.0%로 가장 낮게 나타났다(표 4-33 참조)

〈표 4-32〉 병원급 조사응답기관의 홈페이지 수집항목 및 본인인증 항목 현황

(단위: 개소, %)

구분		응답 병원 수	%
계		105	100.0
수집항목	이름	87	83.7
	주민등록번호	35	33.7
	주소	68	65.4
	전화번호	80	76.9
	이메일 주소	75	72.1
사용 인증수단	주민등록번호	34	32.7
	아이핀(i-PIN)	27	26.0
	신용카드 인증	5	4.8
	공인 인증	13	12.5
	휴대폰 인증	18	17.3

〈표 4-33〉 병원급 조사응답기관의 개인정보처리시스템에 대한 항목별 수행현황

(단위: 개소, %)

구분	계		예		아니오		모르겠음	
	병원수	%	병원수	%	병원수	%	병원수	%
평균				59.5		26.8		13.7
업무권한 차등부여	105	100.0	88	83.8	10	9.5	7	6.7
인사이동에 따른 접근권한 변경 또는 말소	105	100.0	89	84.8	9	8.6	7	6.7
접근권한 내역기록 및 최소 3년간 보관	105	100.0	52	49.5	36	34.3	17	16.2
취급자 접속기록 생성	105	100.0	56	53.3	32	30.5	17	16.2
취급자 접속기록 6개월이상 보관 및 관리	105	100.0	48	45.7	38	36.2	19	18.1
접속기록 점검 및 후속조치	105	100.0	42	40.0	44	41.9	19	18.1

보안조치 상황에 있어서 92.4%가 보안프로그램을 설치 및 업데이트 하고 있으며 비밀번호, 고유식별번호, 바이오정보에 대해서는 각각 69.5%, 59.0%, 13.3% 암호화를 수행하고 있었다. PC내 개인정보 암호화를 위한 소프트웨어는 50.0%가 사용, 이때 비밀번호 작성규칙에 대해서는 57.1%가 준수하고 있었으며 개인정보 기록물에 대해 안전한 장소에 보관하는 경우는 74.3%로 나타났다(표 4-34 참조).

〈표 4-34〉 병원급 조사응답기관의 보안조치 현황

(단위: 개소, %)

구분		계		예		아니오		모르겠음	
		병원수	%	병원수	%	병원수	%	병원수	%
보안프로그램 설치 및 정기적인 업데이트		105	100.0	97	92.4	4	3.8	4	3.8
암호화	고유식별정보	105	100.0	626	59.0	32	30.5	11	10.5
	바이오정보	105	100.0	14	13.3	63	60.0	28	26.7
	비밀번호	105	100.0	73	69.5	24	22.9	8	7.6
PC 내 개인정보 암호화를 위한 소프트웨어 사용		105	100.0	53	50.0	43	41.0	9	8.6
개인정보 송수신의 경우 암호화 여부		105	100.0	38	36.2	50	47.6	17	16.2
비밀번호 작성규칙 수립 및 준수여부		105	100.0	60	57.1	39	37.1	6	5.7
개인정보 기록물에 대한 안전한 보관		105	100.0	78	74.3	16	15.2	11	10.5

사. 개인정보보호 업무수행

병원의 개인정보보호업무 담당자로서 생각하는 우리나라 의료기관과 담당자 본인이 근무하는 해당 병원에 대한 영역별 개인정보보호 관리수준 정도를 파악해본 결과, 우리나라 의료기관의 개인정보보호 관리수준에서 전체적인 수준은 5점 만점에 2.66점으로 생각하고 있었으며 본인

병원에 대해서는 전체적인 수준을 2.98점으로 생각하고 있어 그리 높지 않은 것으로 생각하고 있었다(표 4-35 참조).

〈표 4-35〉 영역별 개인정보보호 관리수준에 대한 병원 개인정보보호업무 담당자의 인지도 현황

(단위: 점)

구분	영역	개인정보보호 관리수준
우리나라 의료기관 수준	관리체계 구축 영역	2.63
	보호대책 수립 및 시행 영역	2.60
	침해사고 대책 영역	2.53
	개인정보처리 영역	2.80
	안전성 확보조치 영역	2.70
	전체 수준	2.66
귀 병원 수준	관리체계 구축 영역	3.02
	보호대책 수립 및 시행 영역	3.04
	침해사고 대책 영역	2.84
	개인정보처리 영역	3.06
	안전성 확보조치 영역	3.03
	전체 수준	2.98

의료기관 개인정보보호 수준향상을 위해 병원의 개인정보보호업무 담당자들은 CEO(의료기관 최고 결정권자), 의료기관 직원, 개발업체 직원, 소비자(환자) 각 대상의 인식제고 중요도에 대한 생각에서 5점 만점에 평균 4.27점으로 나타났으며 CEO, 의료기관직원, 개발업체 직원, 그리고 소비자가 각각 4.50점, 4.31점, 4.26점, 4.01점 순으로 모두 높게 나타나 모든 대상들의 인식제고가 중요한 것으로 판단하고 있었다(표 4-36 참조).

또한 병원 개인정보보호업무 담당자들이 생각하는 국가차원의 지원방법 종류별 중요도는 5점 만점에 평균 4.31점으로 모두 높은 정도를 나타내고 있었다(표 4-37 참조).

〈표 4-36〉 병원 개인정보보호업무 담당자들이 생각하는 대상별 인식제고에 대한 중요도 현황

(단위: 점)

구분	중요도
평균	4.27
CEO(의료기관 최고 결정권자)	4.50
의료기관 직원	4.31
개발업체 직원	4.26
소비자(환자)	4.01

〈표 4-37〉 병원 개인정보보호업무 담당자들이 생각하는 국가차원의 지원방법별 중요도 현황

(단위: 점)

구분	중요도
평균	4.31
기술적 지원(솔루션 도입 등)	4.50
국가차원의 적극적 홍보	4.30
개인정보보호 관련교육	4.31
의료기관용 가이드라인 배포	4.27
개선방안을 위한 자문 지원(컨설팅 등)	4.20

다음으로 개인정보 유출시 개인정보처리자가 해당 정보주체에게 알려야 하는 사항, 영상정보처리기기 관리방안, 개인정보보호책임자가 수행하여야 하는 개인정보처리에 관한 관리·감독 역할, 기술적·관리적 보호조치 기준의 의무규정 각각에 대한 정답률은 80.0%, 82.9%, 47.6%, 94.2%로 개인정보처리에 관한 관리·감독 역할에 대한 세부사항에 대한 인지정도가 상대적으로 낮은 것으로 나타났다.

마지막으로 의료기관 개인정보보호 관리에 있어 일선에서의 어려운 점 혹은 정부에 바라는 점에 대한 주관식 문항에서는 인력지원과 예산투자, 체계적인 교육, 상세한 가이드라인 제공, 의료현장에 적용가능한 보다 완

화된 규제 적용등 순으로 의견을 제시하였다.

3. 의료기관 홈페이지 개인정보처리방침 관리현황

조사대상 의료기관 30,000여 기관에 대해 8월 1일부터 10월 18일까지 약 2달 반 기간동안 분석한 결과, 그 중 홈페이지를 개설·운영하고 있는 기관은 과반수(50.9%) 정도로 나타났으며 병원유형별로는 상급종합병원이 43개기관 모두, 종합병원, 병원, 의원급은 각 73.0%, 61.7%, 50.0%로 나타났다. 이들 홈페이지에 개인정보 처리방침을 게재하고 있는 경우는 홈페이지 운영기관 중 51.4%에 그치고 있었다[24]. 의료기관 종류별로는 상급종합병원이 90.7% 종합병원, 병원, 의원이 각각 81.6%, 63.1%, 50.1%를 나타냈다(표 4-38 참조). 그러나 의료기관에 따라서는 '개인정보 처리방침'을 '개인정보 취급방침', '개인정보 보호정책' 등 다양한 용어를 사용하여 게재하기도 하였다.

〈표 4-38〉 의료기관 종류별 홈페이지 운영 및 개인정보처리방침 게재 현황

(단위: 개소, %)

구분	계	홈페이지 개설 및 운영		처리방침 게재	
		기관수 (개소)	운영률 (%)	기관수 (개소)	게재율 (%)
계	30,082	15,305	50.9	7,869	51.4
상급종합병원	43	43	100.0	39	90.7
종합병원	282	206	73.0	168	81.6
병원	1,435	886	61.7	559	63.1
의원	28,322	14,170	50.0	7,103	50.1

24) 개인정보 처리방침은 홈페이지 뿐 아니라 사무소등 장소에 게시, 간행물, 관보 등에 게재하는 등의 방법을 통해 공개할 수 있으므로 실제 개인정보 처리방침을 수립하여 공개하는 기관은 더 많을 것으로 예측할 수 있음.

다음으로 필수기재사항 10개 항목이 게시되어 있는지를 의료기관 종류별로 살펴본 결과, 분석대상 전체 의료기관에 있어서는 처리목적(98.4%), 처리항목(97.0%), 처리 및 보유기간(96.0%), 보호책임자사항(90.0%), 제3자제공사항(88.5%), 권리및의무사항(84.7%), 파기사항(83.7%), 위탁사항(80.9%), 방침변경사항(80.5%), 안전성확보조치사항(75.5%) 순으로 많이 게시하고 있었다. 그러나 게시내용을 보다 구체적으로 분석해본 결과 내용의 충분성에 있어서는 처리항목(95.0%), 제3자제공사항(85.9%), 파기사항(81.1%), 위탁사항(78.5%), 처리 및 보유기간(75.0%), 방침변경사항(73.3%), 처리목적(63.1%), 안전성확보조치사항(62.7%), 권리 및 의무사항(36,2%), 보호책임자사항(23.0%) 순으로 나타나 특히 보호책임자사항과 권리 및 의무사항에 대한 게시내용에 있어서는 제대로 다루어지지 못하고 있는 것을 알 수 있었다(표 4-39 참조).

'개인정보 처리방침'이라는 용어를 제대로 사용하지 못한 결과에서도 나타난 바와 같이 이는 의료기관들이 각 조항에 대한 이해없이 적용한 결과로 판단되는 바, 향후 이들 의료기관 유형별 정확한 지침 제공과 아울러 각 항목에 대한 이해수준을 높일 수 있는 방안을 강구할 필요가 있다.

4. 일반국민의 개인(의료)정보보호 인식현황

일반국민 대상의 개인의료정보보호에 대한 인식조사는 건강관련 포털 3개(건강정보광장, 금연길라잡이, 건강길라잡이) 및 본 연구원 홈페이지 이용자를 대상으로 2013년 9월 27일 ~ 2013년 10월 10일까지 14일간 온라인 설문조사형태로 실시하였으며 총 3,230명이 참여하였으나 응답내용이 불성실한 것을 배제하고 2,730건을 최종 분석 자료로 사용하였다.

수집된 자료는 SPSS 21 통계프로그램을 활용하여 통계처리 하였으며,

변수에 관한 빈도분석, 교차분석, 기술통계분석, 다중응답분석(multiple response) 등을 실시하였다.

〈표 4-39〉 의료기관 종류별 개인정보처리방침 게시항목 현황

(단위: %)

게시항목	계			상급 종합병원			종합병원			병원			의원		
	소계	완전	미흡	소계	완전	미흡	소계	완전	미흡	소계	완전	미흡	소계	완전	미흡
처리목적	98.4	63.1	35.4	94.9	92.3	2.6	98.8	98.2	0.6	97.3	95.5	1.8	98.6	57.3	41.3
처리 및 보유기간	96.0	75.0	21.0	84.6	43.6	41.0	92.2	48.2	44.0	90.3	60.1	30.2	97.0	78.1	18.8
제3자 제공사항	88.5	85.9	2.6	97.4	92.3	5.1	89.9	88.7	1.2	81.1	79.1	2.0	89.3	86.6	2.7
위탁사항	80.9	78.5	2.4	84.6	84.6	0.0	72.0	72.0	0.0	66.7	65.3	1.4	83.0	80.3	2.7
권리, 의무사항	84.7	36.2	48.5	94.9	84.6	10.3	87.5	82.1	5.4	83.2	61.4	21.8	84.7	30.8	53.9
처리항목	97.0	95.0	2.0	92.3	92.3	0.0	97.0	97.0	0.0	90.9	90.5	0.4	97.8	95.6	2.3
파기사항	83.7	81.1	2.6	79.5	79.5	0.0	78.6	78.0	0.6	73.5	71.0	2.5	85.3	82.5	2.7
보호책임자 사항	90.0	23.0	67.0	89.8	66.7	23.1	88.1	47.0	41.1	86.0	34.3	51.7	90.6	20.3	70.4
방침변경 사항	80.5	73.3	7.2	84.7	82.1	2.6	85.7	79.2	6.5	82.3	69.6	12.7	80.0	73.5	6.5
안전성 확보조치 사항	75.5	62.7	12.8	82.1	82.1	0.0	63.1	63.1	0.0	61.9	61.5	0.4	77.6	62.7	15.0

가. 응답자 특성

분석대상 응답자 수는 2,730명으로 남성 54.0%, 여성 46.0% 분포를 나타내고 있다. 연령대로는 30대(45.1%), 20대(25.1%), 40대(21.1%) 순이었으며 결혼상태는 미혼 53.4%, 기혼이 44.6%, 직업군은 사무직 35.4%, 전문/관리직 15.4%, 서비스/판매직 11.8% 순으로 나타났다(표 4-40 참조).

〈표 4-40〉 일반국민 응답자의 일반적 특성

(단위: 명, %)

구분		응답자수	%
성	계	2,730	100.0
	남자	1,475	54.0
	여자	1,255	46.0
연령대	계	2,730	100.0
	10대	30	1.1
	20대	684	25.1
	30대	1,231	45.1
	40대	576	21.1
	50대	154	5.6
	60대 이상	55	2.0
최종학력	계	2,730	100.0
	중졸이하	38	1.4
	고졸	642	23.5
	대졸	1,878	68.8
	대학원 재학 이상	172	6.3
결혼상태	계	2,730	100.0
	미혼	1,457	53.4
	기혼	1,217	44.6
	기타	56	2.1
직업	계	2,730	100.0
	전문/관리직	420	15.4
	사무직	963	35.3
	서비스/판매직	321	11.8
	생산관련직	122	4.5
	전업주부	318	11.6
	학생	240	8.8
	무직/기타	346	12.7

나. 의료기관 이용특성

최근 1년간 의료기관을 이용한 응답자들이 주로 이용한 의료기관으로는 병원이 53.6%로 가장 많았으며 의원(24.3%), 종합병원(19.1%) 순으로, 이들의 이용횟수는 연간 1~4회 39.3%, 연간 5~11회 23.1%, 월 1회 18.2%, 월2~3회 13.6% 순으로 나타났다(표 4-41 참조).

〈표 4-41〉 일반국민 응답자가 주로 이용한 의료기관 유형 및 이용횟수

(단위: 명, %)

구분			응답자 수	%
계			2,730	
의료기관 이용하지 않음			267	
의료기관 이용	주 이용 기관	소계	2,463	100.0
		종합병원	469	19.1
		병원	1,321	53.6
		의원	598	24.3
		보건의료기관	75	3.0
의료기관 이용횟수	계		2,463	100.0
	월 4회 이상		143	5.8
	월 2~3회		335	13.6
	월 1회		448	18.2
	연간 5~11회		570	23.1
	연간 1~4회		967	39.3

다. 개인의료정보보호에 대한 인식

개인정보 보호법에 대해 일반국민들이 어느 정도 알고 있는지를 물어본 결과, 46.0% 가 들어는 보았으나 잘 알지 못하였거나 전혀 들어본 적이 없다고 답하였으며 16.4% 정도만이 어느정도 혹은 잘 알고 있다고 답하여 아직도 일반국민들은 개인정보 보호법에 대해 제대로 잘 알고 있지는 않는 것으로 나타났다(표 4-42 참조).

〈표 4-42〉 개인정보 보호법에 대한 일반국민들의 인지도 현황

(단위: 명, %)

구분	응답자수	%
계	2,730	100.0
전혀 들어본 적 없다	167	6.1
들어는 보았으나, 잘 알지 못한다	1,089	39.9
대충 알고 있으나 다른사람에게 설명할 수준은 아니다	1,025	37.5
알고 있으며, 다른사람에게 간략히 설명할 수 있는 수준이다	405	14.8
정확하게 알고 있으며, 다른 사람에게 상세히 설명할 수 있는 수준이다	44	1.6

다음으로 개인정보 보호법 관련하여 일반국민들이 누릴 수 있는 권리, 즉 개인정보 처리에 관한 정보를 제공받을 권리, 개인정보 처리에 관한 동의 여부 및 범위를 선택할 권리, 개인정보 처리여부 확인 및 열람을 요구할 수 있는 권리, 개인정보 처리에 대한 정지·정정·삭제·파기를 요구할 수 있는 권리, 신속하고 공정한 절차에 따라 구제받을 권리 등 5개 권리에 대해 알고 있는지 물어본 결과, 5개 권리에 대해 평균 57.7%가 알고 있었으며 그 중 개인정보 처리정보를 제공받을 권리에 대해 가장 많이 알고 있고(76.3%), 구제받을 권리에 대해 가장 잘 모르고 있었다(45.8%)(표 4-43 참조).

개인정보를 일반적인 개인정보(이름, 주민등록번호, 전화번호등), 의료기관 이용에 의해 생성·관리되는 개인의무기록정보, 국민건강보험공단 등 공공기관에 의해 생성·관리되는 개인건강관리정보(건강검진정보 등), 건강포털 이용에 의해 생성·관리되는 개인건강관리정보, 건강관련 모바일 앱 이용에 의해 생성·관리되는 개인건강관리정보 등으로 나누었을 때 각각에 대한 개인정보보호 중요도를 조사한 결과, 5점 만점에 평균 4.25점을 나타냈으며 일반 개인정보, 개인의무기록정보, 공공기관에 의한 개인

건강관리정보, 건강포털에 의한 개인건강관리정보, 모바일앱에 의한 개인건강관리정보 순을 나타냈다(표 4-44 참조)

〈표 4-43〉 개인정보보호 관련 권리에 대한 일반국민들의 인지도 현황

(단위: 명, %)

구분	계		알고 있음		모르고 있음	
	응답자수	%	응답자수	%	응답자수	%
평균		100.0		57.7		42.3
개인정보 처리정보 제공받을 권리	2,730	100.0	2,084	76.3	646	23.7
개인정보 처리 동의여부 및 범위 선택 권리	2,730	100.0	1,792	65.6	938	34.4
개인정보 처리여부 확인 및 열람 요구 권리	2,730	100.0	1,377	50.4	1,353	49.6
개인정보 처리 정지·정정·삭제·파기 요구권리	2,730	100.0	1,378	50.5	1,352	49.5
신속하고 공정한 절차에 따라 구제받을 권리	2,730	100.0	1,250	45.8	1,480	54.2

〈표 4-44〉 항목별 개인정보보호 중요도에 대한 일반국민들의 인지도 현황

(단위: 명, %)

구분	중요도
평균	4.25
일반개인정보	4.42
개인의무기록정보	4.32
공공기관에 의한 개인건강관리정보	4.29
건강포털에 의한 개인건강관리정보	4.17
모바일앱에 의한 개인건강관리정보	4.07

또한 일반적인 개인정보보호, 병원급 의료기관에서의 개인의무기록정보 보호, 의원급에서의 개인의무기록정보 보호, 공공기관에서의 개인건강관리정보 보호, 건강포털에서의 개인건강관리정보 보호, 건강관련 모

바일앱에서의 개인건강관리정보 보호 각각에 대한 관리수준에 대한 생각에서 6가지 항목 모두 5점 만점에 3점 이하로 높지 않은 수준으로 나타났으며(평균 2.49점) 그 중에서는 공공기관에서의 보호수준을 높게 생각하고 있었다(표 4-45 참조). 앞 문항과 연결하여 보았을 때 일반개인정보를 가장 중요하게 생각하는 반면 일반개인정보 보호 관리수준은 가장 낮다고 생각하여 일반국민들은 우리나라의 일반개인정보 보호 관리수준에 대해 우려하고 있는 것으로 생각해볼 수 있을 것이다.

〈표 4-45〉 항목별 개인정보보호 관리수준에 대한 일반국민들의 인지도 현황

(단위: 점)

구분	개인정보보호 관리수준
평균	2.49
일반개인정보 보호	2.31
병원에서의 개인의무기록정보 보호	2.55
의원에서의 개인의무기록정보 보호	2.48
공공기관에서의 개인건강관리정보 보호	2.70
건강포털에서의 개인건강관리정보 보호	2.47
모바일웹에서의 개인건강관리정보 보호	2.41

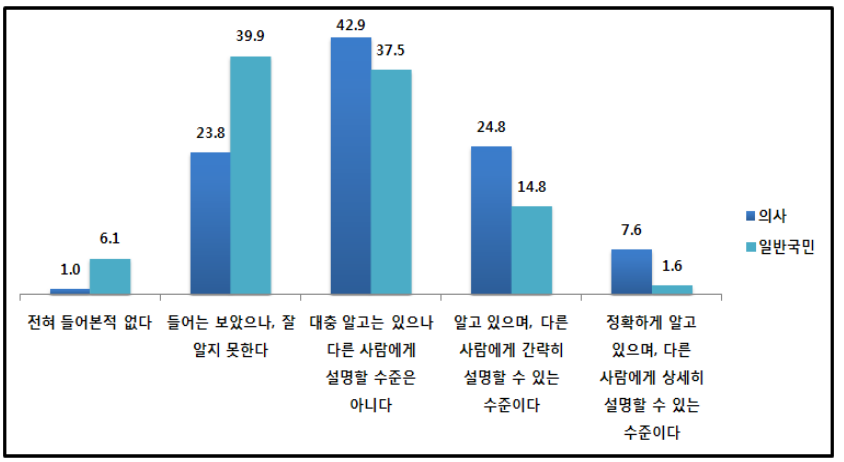
마지막으로 개인건강정보보호에 있어 정부 혹은 관련기관에 바라는 점에 대한 주관식 문항에서는 의원, 병원등 의료기관에서 의료현장에 맞는 보다 완화된 규제를 적용해 달라는 요청과는 달리 개인정보보호에 대한 제도적 혹은 정책적 강화, 보다 안전한 개인정보처리에 대한 요청, 개인정보 유출사고나 오남용 발생시 피해보상 혹은 처벌 강화, 보다 적극적인 홍보 등 대부분은 현재보다 강화되기를 바라고 있었으며 일부이기는 하나 개인정보에 대한 수집 및 서비스신청의 편리성을 위해 현재수준보다 완화를 원하는 의견도 있었다.

5. 소결 및 시사점

본 절에서는 앞에서 기술한 의원(의사), 병원, 의료기관 홈페이지 개인정보처리방침, 일반국민에 대해 분석한 결과에 대해 각 항목별로 의원(의사), 병원, 일반국민, 의사 vs. 일반국민, 의원 vs. 병원 등으로 다시한번 간단하게 비교정리하고 이에 대한 시사점을 밝히고자 한다.

첫째, 개인정보 보호법에 대한 의사 vs. 일반국민의 인지정도에서는 일반국민보다는 의사군의 인지정도가 더 높게 나타났다(그림 4-1 참조). 이는 아무래도 의사들은 현장에서 개인정보를 직접 취급하는 당사자이므로 개인정보주체인 일반국민보다는 인지정도가 더 높은 것으로 판단되며, 그러나 아직도 일반국민들은 개인정보보호에 대한 중요성과 필요성, 그리고 구체적인 내용에 대한 이해가 부족한 것으로 판단되어 이에 대한 홍보가 필요하리라 생각된다.

〔그림 4-1〕 개인정보 보호법에 대한 인지정도(의사 vs. 일반국민)



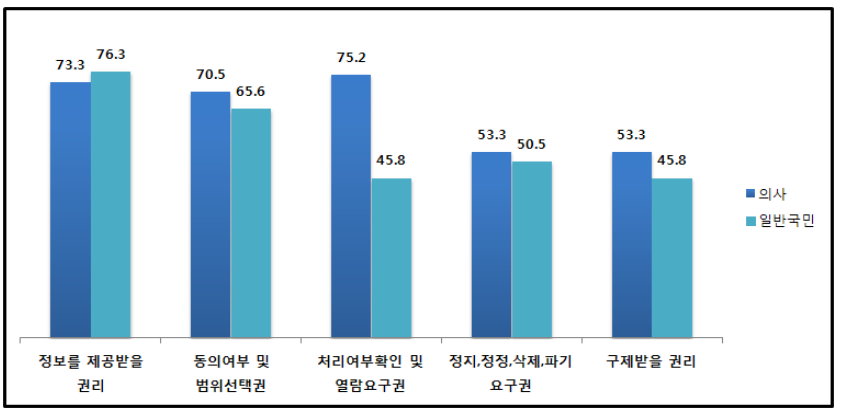
둘째, 홈페이지 운영에 있어 의원과 병원 모두 외부에 위탁하는 경우가 많았는 바, 이는 외부위탁 시 개인정보보호에 대한 중요성에 대한 인지와 더불어 철저한 관리가 필요한 대목이라 할 수 있다. 그러나 업무위탁시 문서화 필요사항과 수행업무에 대해 특히 의원급에서는 각각 45.2%, 50.8%의 낮은 인지도를 나타내고 있어 이에 대한 인지제고와 더불어 철저한 관리가 필요하다 하겠다.

셋째, 개인의료정보보호 관련 예산책정에 있어(병원급) 단기간 효과가 나타나는 혹은 보다 적용이 용이한 HW, SW 도입에 대한 책정비율이 높고, 상대적으로 컨설팅, 모니터링, 교육, 홍보 등을 위한 예산책정비율이 낮았으며 민간병원보다 공공병원에서 HW, SW 도입에 대한 예산책정비율이 높았는 바, 이는 앞으로 정부가 컨설팅, 모니터링, 교육, 홍보 부문에 대한 대응방안을 보다 적극적으로 강구할 필요를 나타낸 것이라 볼 수도 있다.

넷째, 개인의료정보보호 관련 교육과 관련하여 의사군 및 병원에서 필요로 하는 자료는 실 업무에 맞는 사례중심의, 규제중심의, 필수사항에 대한 내용으로써, 의사들이 정보 취득처로 많이 활용하는 것은 관련 협·단체, 동료, 인터넷 검색 등이므로 향후 사례중심의 맞춤형 교육콘텐츠를 개발하고 이를 보급시에는 관련 협·단체를 통해, 그리고 보도자료, 인터넷 홈페이지 등을 통한 배포방안을 강구할 필요가 있다.

다섯째, 정보주체권리 중 동의여부 및 범위선택권, 처리여부 확인 및 열람요구권, 구제받을 권리에서는 일반국민보다는 의사군에서 인지정도가 더 높게 나타났으며 정보제공받을 권리, 정지·정정·삭제·파기 요구권에 대해서는 의사군보다 일반국민의 인지정도가 더 높게 나타났다. 특히 동의여부 및 범위선택권, 처리여부확인 및 열람요구권, 구제받을 권리와 같은 내용은 일반국민의 인지정도가 50% 정도로 향후 이에 대한 홍보가 더 필요할 것으로 생각된다(그림 4-2 참조).

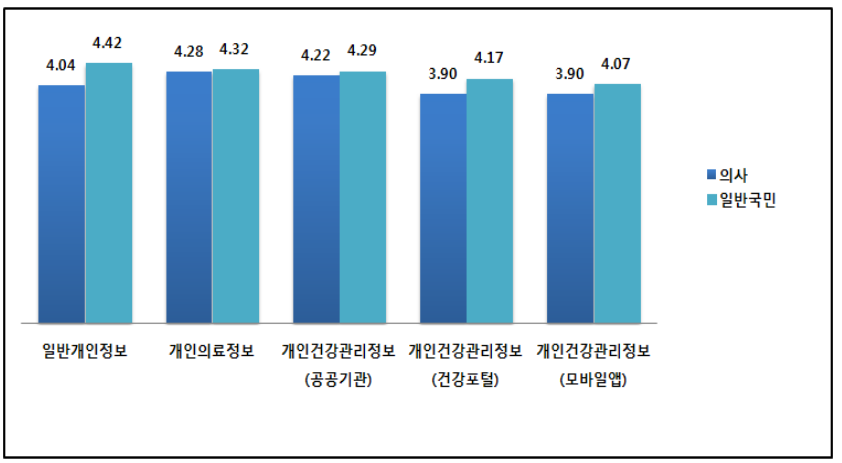
〔그림 4-2〕 정보주체권리에 대한 인지정도(의사 vs. 일반국민)



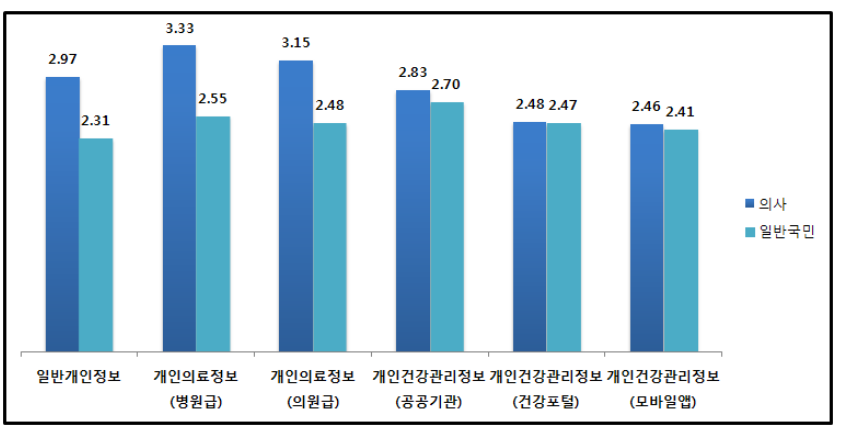
여섯째, 개인정보 중요도에 대해서는 전체적으로 의사군보다 일반국민들이 더 중요하게 생각하고 있었으며 그 중에서도 일반개인정보, 개인건강관리정보(건강포털, 모바일앱)에 대해 두 군간의 많은 차이를 보이고 있다(그림 4-3 참조).

일곱째, 개인정보 관리수준에 대한 인지정도에 있어서는 의사군, 일반국민 모두 중요도에 비해 관리수준이 낮다고 평가하고 있었으며 개인정보 종류별로는 일반개인정보에 대한 관리, 병원급에서의 개인의료정보관리, 의원급에서의 개인의료정보 관리, 공공기관에서의 개인건강관리정보 관리수준에 대해서는 의사군이 일반국민보다 더 높게, 건강포털에서의 개인건강관리정보 관리, 모바일앱에서의 개인건강관리정보 관리에 대해서는 의사군과 일반국민의 인지정도가 거의 비슷하게 낮게 나타났다(그림 4-4 참조). 이러한 결과로 볼 때 의사군은 의료기관에서의 개인정보 관리수준에 대해 일반국민이 생각하고 있는 것보다는 더 높게 평가하고 있으며 반면 건강관리를 위한 건강포털 및 모바일앱에서의 관리수준에 대해서는 의사군, 일반국민 모두 낮게 생각하고 있어 향후 이에 대한 대책마련이 필요하다 하겠다.

〔그림 4-3〕 개인정보 중요도에 대한 인지정도(의사 vs. 일반국민)



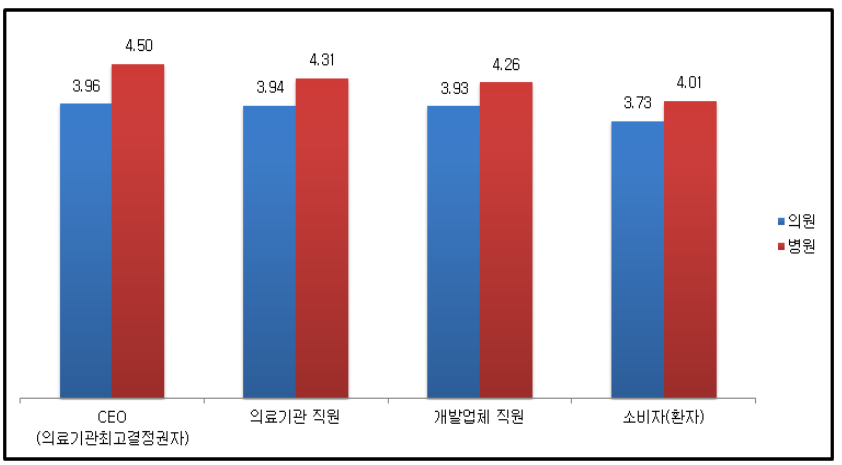
〔그림 4-4〕 개인정보 관리수준에 대한 인지정도(의사 vs. 일반국민)



여덟째, 개인정보 보호 인식제고 대상의 중요도에 대한 의원 vs. 병원 분석결과에서는 의료기관의 CEO, 의료기관 직원, 개발업체 직원, 소비자 4개 항목 모두 의원보다 병원에서 더 중요하게 생각하는 것으로 나타

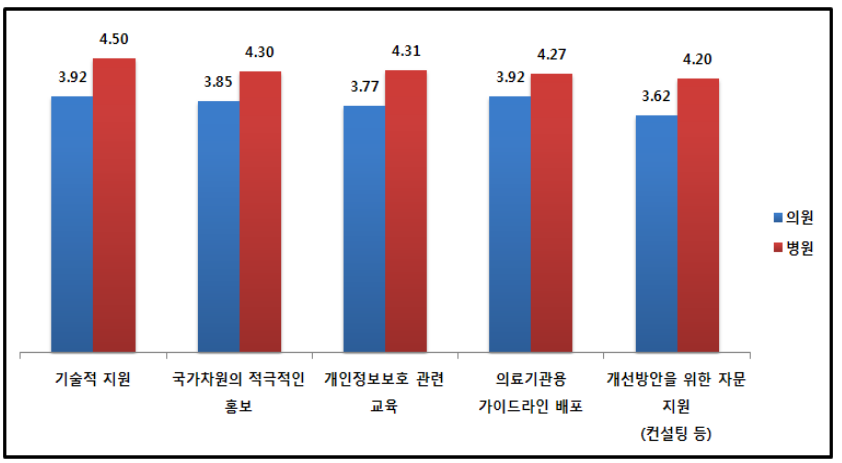
났으며 의원과 병원 모두 개인의료정보주체인 소비자(환자)보다는 의료기관의 CEO, 의료기관 및 개발업체 직원 등 소비자의 개인의료정보를 다루는 의료기관 관계자들의 중요도가 더 높게 나타나 이들의 인식제고가 더 필요하다고 생각하는 것으로 판단할 수 있다(그림 4-5참조).

[그림 4-5] 개인정보 보호 인식제고 대상의 중요도(의원 vs. 병원)



아홉째, 국가차원의 개인정보 보호 지원방법별 중요도에서는 기술적 지원, 국가차원의 적극적인 홍보, 개인정보보호관련 교육, 의료기관용 가이드라인 배포, 자문(컨설팅) 지원 등 모든 항목에서 의원보다 병원에서 더 중요하게 생각하는 것으로 나타났다(그림 4-6 참조).

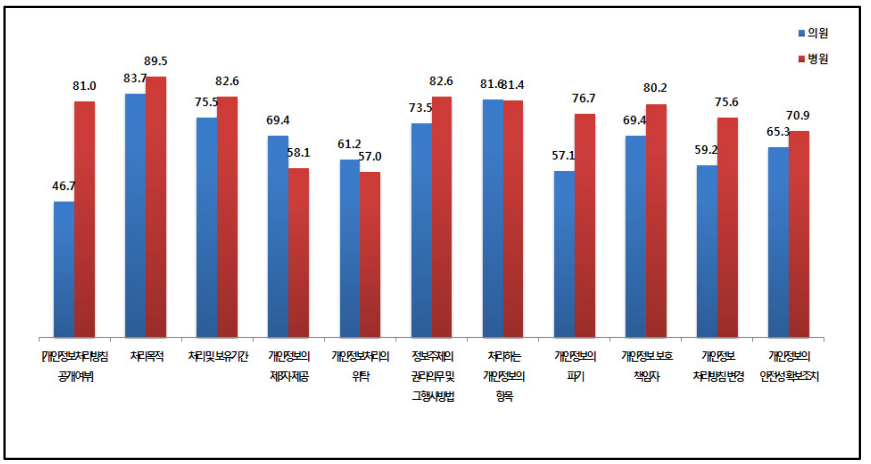
〔그림 4-6〕 국가차원의 개인정보 보호 지원방법별 중요도(의원 vs. 병원)



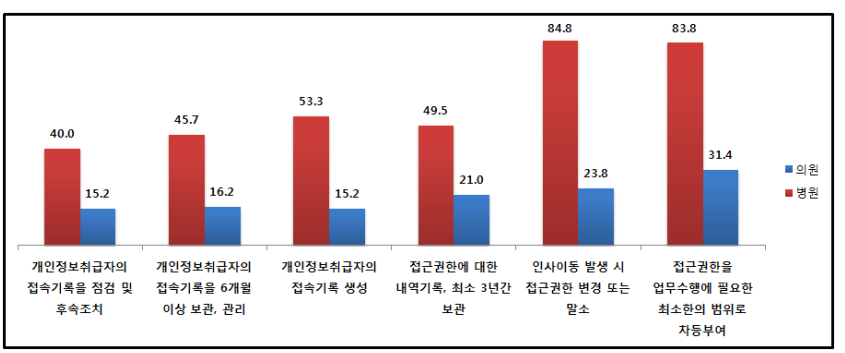
열 번째,개인정보처리방침에 대한 공개 및 개별항목에 대한 공개 여부에서는 의원급이 46.7%, 병원급이 81.0%로 전체적으로 볼때 의원급에서 공개정도가 낮고(그림 4-7 참조), 실제 홈페이지를 대상으로 필수 기재사항 10개 항목 내용의 충분성에 대해 분석해본 결과에서는 미흡한 내용들이 많이 나타난 바, 이는 의료기관들이 각 조항에 대한 충분한 이해없이 적용한 결과로 판단되어 향후 이들 의료기관 유형별 정확한 지침 제공과 아울러 각 항목에 대한 이해수준을 높일 수 있는 방안을 강구할 필요가 있다 하겠다.

열한번째, 개인정보 안전성 확보조치에서는 의원급과 병원급을 비교해 보았을 때, 의원급에서의 조치가 상대적으로 매우 낮은 것을 알 수 있다(그림 4-8 참조). 이는 향후 의료기관에 대한 홍보, 교육시 특히 의원급을 대상으로 안전성 확보조치에 대한 내용을 강화할 필요가 있다 하겠다.

〔그림 4-7〕 개인정보처리방침 개별항목에 대한 공개 여부(의원 vs. 병원)

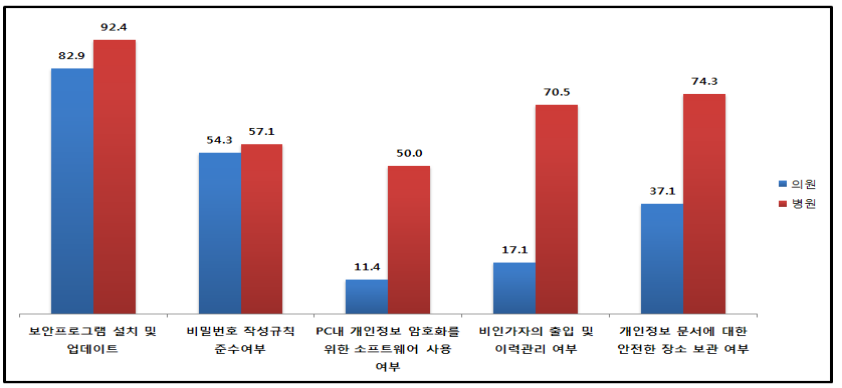


〔그림 4-8〕 개인정보처리시스템에 대한 안전성 확보조치 수행현황(의원 vs. 병원)



열두 번째, 각 기관의 보안조치 상황에서도 병원급이 상대적으로 의원급보다 많이 이행하고 있는 것으로 나타났다. 특히 개인정보문서에 대한 보관, 비인가자 관리, PC내 암호화 소프트웨어 사용 항목에 있어서 의원급의 이행정도가 매우 낮아 향후 이에 대한 대책마련이 필요하다 하겠다(그림 4-9 참조).

〔그림 4-9〕 보안조치 현황(의원 vs. 병원)



마지막으로 의원급, 병원급 모두 정부에게 바라는 점에 대해서는 보다 의료현실과 의료현장에 적합한 완화된 규제 적용, 체계적인 교육 실시, 상세한 가이드라인 제공, 인력지원과 예산 투자, 그리고 주민번호 대체방안 강구 등을 제시하고 있는 바, 이는 앞에서 나타난 여러 가지 현황에서 나타난 시사점과 더불어 개선방안을 마련함에 있어 참고할 수 있다 하겠다.

제5장 결론 및 정책적 제언

제1절 결론

제2절 정책제언

5 결론 및 정책적 제언

제5장에서는 제2장, 제3장 및 제4장에서 분석한 각종 개념, 제도 및 의료기관의 개인의료정보 보호관리현황과 인식현황을 기반으로 본 연구의 결론 및 정책방안을 제시하였다.

제1절 결론

본 절에서는 제2장, 제3장 및 제4장에서의 주요 논점 및 시사점 등을 정리하여 결론을 도출하였다.

첫째, 개인의료정보 보호의 중요성과 시의성

개인정보는 시대와 기술, 그리고 사람들의 인식이 변화하면서 그 적용대상과 범위도 변화하기 마련이다. 그 중에서 의료기관을 중심으로 수집, 이용, 관리되는 개인의료정보는 정보기술이 발달하면서 이용, 활용가치도 증가하였으나 반면, 접근경로와 이동성이 증가하면서 개인정보 유노출, 개인정보 침해와 같은 정보화 역기능도 중요사회문제로 부각되었다. 2011년 3월 「개인정보 보호법」이 제정을 계기로 개인정보 보호, 의료기관에서의 개인의료정보 보호의 중요성과 필요성, 그리고 이를 위한 일련의 필요활동에 대해 되짚어볼 시점에 이르렀다.

둘째, 개인정보 보호관련 법규제 강화에 따른 개인의료정보 보호 관리방안

최근 개인정보 보호관련 법·제도는 국내의 '개인정보 보호법' 개정으로

인한 규제 강화 뿐 아니라 국제적인 교류에 있어서도 점차 강화되고 영역별로 상세화되어 가는 추세에 있어 의료영역에 대한 보다 집중적인 관심과 관리방안 마련이 필요하나 이를 위해 정확한 실태를 파악할 수 있는 의료기관 및 의료인을 대상으로 한 주기적인 실태조사가 없는 실정이다.

셋째, 개인의료정보 보호를 위한 자율규제 실천

개인정보 보호를 위해서는 법적 규제 뿐 아니라 자율규제적 성격의 인증제도 정착과 활성화가 필요하나, 기존 개인정보보호 인증제도 내에서는 의료영역에 대한 개인의료정보 보호 관리체계 인증을 위한 특화된 평가기준이 마련되어 있지 않다. 또한 현재의 '의료기관 인증제도' 평가체계 내에 개인의료정보 보호관련 기준항목이 너무 간략하게 마련되어 있어 개인의료정보 보호에 대한 충분한 효과를 나타내지 못하고 있다.

넷째, 개인정보보호 및 개인의료정보보호에 대한 홍보 및 교육, 컨설팅 및 모니터링

개인의료정보 보호에 대한 인식제고 및 수준향상을 위해서는 일반국민, 의료기관 종사자(의료진 및 관계직원), 진료정보시스템 개발업체 직원을 대상으로 개인정보보호, 개인의료정보보호에 대한 중요성과 정보주체의 권리, 정보취급자의 의무, 그리고 각종 규제사항 등에 대한 적극적인 홍보와 교육이 필요할 뿐 아니라 개인의료정보 보호 수준 향상을 위한 컨설팅, 모니터링이 중요한 요소 중의 하나이다. 그러나 현재 각 의료기관 특히 공공 의료기관에서는 이에 대한 예산책정 및 충분한 정보가 미흡한 상황이다.

다섯째, 사례중심의 현장감있는 개인의료정보 보호 관련 콘텐츠

개인정보 보호법을 의료현장에서 적재, 적소, 적시에 올바르게 적용하기 위해서는 사례중심의 다양한 필수 맞춤형 관련콘텐츠가 체계화된 창구를 통해 제공되어야 하나 기관 유형별, 상황별, 업무별 맞춤형 콘텐츠가 미흡할 뿐 아니라 이를 체계적이고 효과적으로 제공해줄 창구가 정립되어 있지 않다.

여섯째, 개인의료정보의 확장된 범위에서의 개인건강정보 보호

의료기관, 공공기관 등에서의 개인의료정보 보호 뿐 아니라 건강관리 서비스를 제공해주고 있는 건강관련포털, 모바일앱에서의 개인건강정보 보호에 대한 이슈도 점차 비중있게 다루어져야 할 것이다.

마지막으로 본 연구의 한계점으로는, 의원급 및 병원급 개인의료정보 보호 관리현황을 파악하기 위해 직접 현장점검 혹은 대면을 통한 실태조사가 아닌 설문지를 통한 온라인 조사 혹은 서면조사를 실시함으로써 조사결과의 정확성이 일부 떨어질 우려가 있다는 것이다. 그 한 예로 본 연구에서의 조사 항목 중 정보시스템(OCS, EMR) 도입현황에 대한 조사문항은 일부 기관담당자를 대상으로 사전 조사를 거쳤음에도 불구하고 본 조사 실시 이후 의료기관별, 응답자별 이해정도가 상이하여 응답에 어려움이 있다는 의견에 따라 최종 분석결과에는 포함하지 않은 것을 들 수 있다. 온라인 조사, 서면 조사 수행시 발생할 수밖에 없는 이러한 한계점은 향후 보다 상세한 설명과 더불어 사전의 여러 관계자와의 긴밀한 협의를 통해 보완해 나갈 수 있을 것이다. 또한 의원급 응답률을 독려하는 과정에서 시도 의사회 정보통신위원회 임원진이 많이 참여하였는 바, 이는 대표성에 대한 문제가 제기될 수 있는 바, 향후 표본추출에 대한 개선점

을 염두에 두어야 할 것이다.

제2절 정책제언

다음으로 문제점, 시사점 등을 종합하여 정책제언을 제시해보면 크게 6가지로 나누어볼 수 있다.

첫째, 의료기관의 개인의료정보 보호 수준향상을 위한 다양한 정책연구를 통해 시의적절한 정책개발이 가능할 것이다.

현재 개인정보 보호 부문에서는 관리적, 기술적, 물리적 방안 뿐 아니라 여러 사용계층에 대한 인식, 행태 등에 관한 다양한 연구가 시도되고 있으나 의료기관, 개인의료정보 보호 관련해서는 최근 활발한 연구가 진행되고 있지 않다. 이는 상대적으로 개인정보 유노출, 침해에 의한 피해가 사회적으로 크게 부각되지 않아 정보주체 및 정보취급자 모두 그 심각성을 실감하지 못한 이유일 수도 있고, 한편으로는 개인의료정보 보호에 대한 전문가 층이 충분히 형성되지 못한 이유일 수도 있다. 그러나 의료기관측면의, 개인의료정보 보호에 대한 필요성과 중요성은 더욱 더 강조해도 지나치지 않을 것이다.

그러므로 '개인정보 보호법' 이후 보다 강화된 규제 속에서 개인의료정보 보호 수준향상을 위해서는 다양한 정책연구와 정책이 개발될 수 있도록 관련 과제발굴과 같은 정부의 뒷받침이 필요하다 할 것이다.

둘째, 의료기관의 개인정보보호 관리현황 및 개인의료정보보호 인식에 대한 통계자료 제공을 위한 주기적인 실태조사를 통해 다양한 정책연구 및 정책개발이 수행될 수 있을 것이다.

의료기관의 개인정보보호 관리수준을 파악하고 이에 대한 문제점과 취약점 등을 정확하게 분석하여 이에 맞는 대안을 모색하기 위해서는 의료기관의 개인정보보호 관리현황에 대한 전반적인 실태파악과 더불어 개인의료정보보호, 개인건강정보보호에 대한 의료기관 종사자, 일반국민의 인식수준 파악이 필요하다. 관련하여 현재 건강보험심사평가원에서는 매년 의료기관 정보화에 대한 실태조사를 수행하고 있으나 개인정보보호 관리현황에 대해서는 1~2개 항목만 포함되어 있어 개인정보보호 관리에 대한 전체적이고도 세부적인 현황 및 문제점, 취약점 등을 파악할 수가 없다. 또한 방송통신위원회와 한국인터넷진흥원이 매년 실시하고 있는 기업 및 개인대상의 정보보호실태조사는 종사자수 5인이상, 네트워크에 연결된 컴퓨터를 1대이상 보유한 전국의 사업체를 대상으로 하므로 주로 종사자수가 5인 미만인 의원급 의료기관의 경우, 해당 조사에서 배제되고 있고, 일반적인 개인정보보호에 대한 인식수준을 파악하고 있어 개인의료정보보호, 개인건강정보보호에 대한 인식수준은 파악할 수가 없는 실정이다. 그러므로 정부 및 공공기관이 주도하여 의료기관 종류별 개인정보보호 관리현황 혹은 개인의료정보 보호, 개인건강정보 보호에 대한 인식을 주기적으로 파악하여 통계자료를 제공할 수 있는 실태조사 마련이 필요하다 할 것이다. 한편 이러한 의료기관 대상의 실태조사는 본 연구 조사에서도 경험하였듯이 참여율이 매우 낮으므로 대한병원협회, 대한한방병원협회, 대한치과병원협회, 대한중소병원협의회, 대한병원정보협회, 대한전문병원협의회 등과 같은 관련 협·단체와 조사설계단계부터 조사분석단계, 정책대안 마련에 이르기까지 같이 참여할 수 있어야 한다. 이러한 주기적인 관리현황 및 인식현황자료에 기반하여 앞에서 제안한 지속적이고도 연속적인 정책연구 및 정책개발을 수행할 수 있을 것이다.

셋째, 의료기관 종류별 맞춤형 필수 관리지침 및 교육콘텐츠 개발, 체계적인 보급창구에서의 적극적인 배포를 통해 개인의료정보 보호에 대한 의료기관 종사자 및 관계자들의 인식수준이 제고되고 궁극적으로 관리수준이 향상될 것이다.

현재 의료기관용 개인정보 보호 가이드라인은 개발, 보급되어 있으나 의원, 병원, 종합병원, 요양병원 등과 같이 의료기관의 특성을 반영하지 않고 일괄 적용하고 있고 개인정보 보호법에 대한 모든 내용을 담고 있다 보니 취약한 영역을 집중해서 다루지 못하고 있다. 특히 올해 하반기에 실시된 개인정보보호 합동점검단의 의료기관(의원급)대상 실태검사에 참여해본 결과, 의원급 의료기관에서는 개인의료정보 유노출, 침해 등에 대한 가능성 및 규제내용에 대한 충분한 이해없이, 부정확하고 불완전한 정보에 의해 대처하고 있었다. 이는 개인정보 보호법 내용에 대한 충분한 인지 기회가 없고 정확한 정보를 제공해 주는 제공체계가 부재함에 기인함을 알 수 있었다. 그러므로 의료기관 개인정보보호 관리실태 현황 등을 통해 나타난 문제점 및 취약점, 그리고 기존 개인정보보호합동점검단의 의료기관대상 실태검사 결과 나타난 현장에서의 문제점 등을 중심으로 의료기관 종류별 맞춤형 필수 관리지침 혹은 교육콘텐츠 개발이 필요하며 개발된 관리지침 및 교육콘텐츠 등은 대한병원협회, 대한의사협회, 중소병의원협의회, 대한병원정보협회, 시도 및 시군구 의사회, 전문과목별 의사회 등 관련 협·단체 등을 통해 혹은 보건복지부문 개인정보보호 창구를 통해 체계적이고 명확한 안내와 함께 적극적인 보급활동 또한 필요할 것이다.

넷째, 의료기관 대상의 개인정보보호 인증제도를 적극 수용하고 이를 위한 문제점 진단 및 기술지원 등 의료기관 종류별 맞춤형 컨설팅을 제공하여 수준 향상을 꾀하고자 한다.

의료기관 대상 개인정보보호 관리에 대한 일정기준에 도달하기 위해서는 먼저, 현재 환자의 안전과 의료서비스의 질 향상을 위한 의료기관 인증제도의 인증기준에 환자의 개인의료정보 보호를 위한 시범항목을 정착하고 점차 확대할 필요가 있다. 또한 올해 말부터 시행예정인 개인정보보호수준 인증제도(PIPL)는 분야별 인증제도를 지향하고 있어 의료기관도 그 적용대상이 되므로 향후 참여유도를 위한 사전 인증에 따른 컨설팅 지원 등과 같은 인센티브 마련도 고려해볼 만 하다. 의료기관은 직원수가 최소 2인으로 구성된 의원급에서부터 직원수가 7,000~8,000 명에 이르는 상급의료기관까지 매우 다양하며 개인정보보호업무 담당자도 의원의 원장 의사선생님에서부터 종합병원의 원무과 직원, 의무기록팀 직원, 홍보과 직원, 전산팀 직원 등 까지 매우 다양한 양상을 띠고 있다. 반면 개인정보보호업무는 관리적, 기술적, 물리적 측면을 다 포함하고 있어 기관에 따라서는 개인정보보호업무에 대한 이해도 차이가 많이 날 수밖에 없다. 그러므로 인증을 신청하기 이전에 이러한 의료기관 특성에 맞는 문제점 진단 및 기술지원 등 맞춤형 컨설팅을 제공하는 방안을 고려해볼 수 있다. 맞춤형 컨설팅은 정부 및 공공기관이 주도하고 대한병원협회와 대한의사협회를 의료기관에 대한 신청접수기관으로 하여 수행한다면 기관별 차별화된 역할분담에 따른 좋은 성과를 낼 수 있을 것이다.

다섯째, 의료부문 개인정보 보호 교육체계 마련을 통한 전문교육 수행 및 전문인력 양성을 기대한다.

현재 한국정보화진흥원에서는 개인정보 보호관련 교육을 시행하고 있을 뿐 아니라 관련전문인력을 양성하기 위한 노력을 기울이고 있다. 반면 의료영역에서는 이러한 역할을 수행하는 기관 및 단체가 없어 개인의료정보보호 관련 교육콘텐츠 개발, 관리, 보급 등이 원활하지 않고, 전문인

력 양성도 기대할 수 없는 실정이다. 그러므로 정부 및 공공기관 주도 하에 의료부문의 전문화된 개인정보 보호 관련 교육수행을 위해 대한병원협회, 대한의사협회, 중소병의원협의회, 대한병원정보협회, 시도 및 시군구 의사회, 전문과목별 의사회 등 관련 협·단체와의 협의체를 통해 관련교육계획을 수립하고 분야별, 영역별 교육을 수행하며 또한 분야별 전문인력을 꾸준히 양성할 필요가 있다.

마지막으로 의료영역에서의 개인정보보호 규제준수를 관리·감독하고 다양한 개인정보 보호 활동 수행을 위한 보건복지분야 개인정보보호 전문기관 육성을 통해 선진화된 보건복지분야 개인정보보호 관리수준 향상을 기대한다.

앞에서 언급한 개인의료정보 보호관련 다양한 정책연구 및 정책개발, 주기적인 실태파악, 맞춤형 관리지침 및 교육콘텐츠 개발·보급, 맞춤형 컨설팅 제공, 교육체계 마련 등을 위해서는 보건복지분야의 별도 전문기관 육성이 필요하다 하겠다. 현재 우리나라에서는 국가적 차원의 개인정보보호와 관련한 기술지원, 현장점검, 공공기관 개인정보보호 수준진단, 개인정보보호 포털 운영, 개인정보침해신고센터 운영, 관련교육, 인증기관 운영 등 다양한 개인정보보호업무 및 활동을 수행하기 위하여 한국인터넷진흥원[25], 한국정보화진흥원[26]이 관련 법에 근거하여 지정되어 있다. 그러나 보건복지분야에는 이를 위한 충분한 예산 및 별도의 전문기관이 지정되어 있지 않아 보다 다양한 활동을 펼치지 못하고 있는 실정이다. 그러므로 개인정보보호 측면에서 특히 중요한 의료분야, 더 나아가 보건복지분야의 개인정보보호 업무 및 다양한 활동을 안정적이고 지속적으로

25) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제52조(한국인터넷진흥원), 동법 제65조(권한의 위임·위탁).
26) 국가정보화기본법 제14조(한국정보화진흥원의 설립등), 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제65조(권한의 위임·위탁).

수행하고 개인정보보호 규제준수를 관리·감독할 수 있는 보건복지분야 개인정보보호 전문기관 육성이 필요하다 하겠다. 이러한 전문기관에 대한 필요요소로는 신뢰성, 전문성, 중립성 및 객관성, 인프라의 안정성, 업무의 지속성 등을 제시할 수 있으며 그 중에서도 보건복지 다양한 분야의 연구 및 정책개발에 대한 전문성과 더불어 중립적이고도 객관적인 제3자적 입장 유지가 중요하다 하겠다.

이상과 같은 6가지 정책제언들은 사실상 총체적인 관점에서 접근한 것으로써, 추후 각각에 대한 보다 심도있는 접근을 통해 개인의료정보 보호 수준에 대한 보다 발전적인 모습을 기대해보고자 한다.

참고문헌

〈문헌〉

건강보험심사평가원(2005.11.29.). 우리나라 의료정보화 수준, 세계 최고 -심평원의 요양기관 종별 정보화 실태조사 결과 -. 건강보험심사평가원 보도자료.

개인정보보호위원회(2012). 2012 개인정보보호 연차보고서.

경북대학교·SK c&c 컨소시엄(2011). 요양기관 정보화 실태조사(최종보고).

김기열(2010). 공고부문에 관한 외국의 개인정보 보호 법제와 국내 입법의 검토 방향. 월간법제, 2010.09.

김동수·김민수(2006). e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책 방향. 정보화정책, 13(4), pp.128~148. 서울: 한국정보화진흥원.

김태한(2003). 정보화사회와 개인정보보호. 정치정보연구, 6(2), pp 1~21. 서울: 한국정치정보학회.

박지용(2012). 환자의 프라이버시 및 정보보호의 법적 근거 고찰. 한국의료법학회지, 20(2), pp163~190. 한국의료법학회.

박윤형(2005). 진료정보와 국민 사생활 보호정책의 현황과 전망. 한국의료법학회지, 13(1), pp87~98. 한국의료법학회.

박형욱(2010). 보건의료연구에서의 진료정보 보호와 공개, 한국의료법학회지, 18(1), pp.129~148. 한국의료법학회.

방송통신위원회(2013.2.22.). "방통위, 2012년 정보보호 실태조사 결과 발표", 방송통신위원회 보도자료.

방송통신위원회·한국인터넷진흥원(2012a). 2012년 인터넷이용실태조사.

방송통신위원회·한국인터넷진흥원(2012b). 2012개인정보보호 실태조사(개인편).

방송통신위원회·한국인터넷진흥원(2012c). 2012개인정보보호 실태조사(기업편).

보건복지부(2012.01). 보건복지부 개인정보보호 기본지침.

보건복지부(2013a). 2013년도 개인정보보호 관리수준 현황조사 제안요청서.

보건복지부(2013b). 보건복지부 내부자료.
보건복지부·의료기관평가인증원(2011a). 2011 의료기관 인증조사 기준집(대형 병원용).
보건복지부·의료기관평가인증원(2011b). 2011 의료기관 인증조사 기준집(중소 병원용).
보건복지부·의료기관평가인증원(2012a). 2013 요양병원 인증조사 기준집.
보건복지부·의료기관평가인증원(2012b). 2013 정신병원 인증조사 기준집.
백윤철(2005). 헌법상 환자의 의료정보에 대한 권리에 관한 연구. 헌법학 연구, 11(3), pp.337~373. 한국헌법학회.
백윤철(2008). 미국의 개인정보보호와 HIPPA. 미국헌법연구, 19(1), pp.53~104. 미국헌법학회.
안전행정부(2013). 2013년 공공기관 개인정보보호 관리수준진단 계획.
안전행정부(2013.7.30.). "공공기관도 주민번호 수집 엄격히 제한". 안전행정부 보도자료.
안전행정부(2013.10.28.). "개인정보 보호법 준수기관, 인증받는다". 안전행정부 보도자료.
안전행정부(2013.12.16.). "2013년도 공공기관 개인정보보호 관리수준진단 결과 공개". 안전행정부 보도자료.
안전행정부·한국인터넷진흥원(2013.07). 2013년 공공기관 개인정보보호 관리수준진단 매뉴얼.
안전행정부·한국정보화진흥원(2013.09.06.). 개인정보 위반사례와 현장 점검결과.
엄현호(2013). 의료기관의 개인정보 보호법 이행현황 및 개선방안에 관한 연구. 가톨릭대학교 보건대학원 석사학위논문.
윤재석(2012.12.12.). OECD 프라이버시 가이드라인 개정현황 및 향후 전망. 주간기술동향 1565호. 정보통신산업진흥원.
이유지(2005). 병원보안 이슈와 과제. 컴퓨터월드, 7월호, pp.71-82.
이인호(2005). 개인정보 보호법의 합리적인 입법기준의 모색. 디지털 정보의 효율적 이용과 프라이버시의 효과적 보호에 관한 정책토론회.

이자성(2007). 일본 개인정보 보호법의 체계 및 구성 내용에 관한 고찰. 전자정부법제연구, 2(1), pp.111~136.

이한주(2012). 의료영역에서의 개인정보보호의 문제점과 해결방안. 한국의료법학회지, 20(2), pp.267~293, 한국의료법학회.

전기홍·조우현(1994). 우리나라 병원정보시스템 실태에 관한 연구. 보건행정학회지, 4(2), pp.1~16. 서울: 한국보건행정학회.

전은정·김학범·염흥열(2012). 유럽의 개인정보보호 법·제도 동향. 정보보호학회지, 22(2), pp58~72.

정보통신부(2007.3.6.). "정통부, 개인정보보호 실태점검 대폭 강화". 정보통신부 보도자료.

정영철·송현종·이견직(2003). 보건의료부문 정보화사업 전략적 평가모형 개발. 서울: 한국보건사회연구원.

정영철·신윤정·정영호·최은진·고숙자·김동수·김정은·이견직·조병희·홍승권(2005). 국내 e-Health 발전에 따른 정책대응방안 연구. 서울; 한국보건사회연구원.

정영철·이야리(2013.11.). 우리나라 의료기관의 개인정보 보호 인증제도 적용을 위한 정책과제. 보건복지포럼, 205, pp.70~86. 한국보건사회연구원.

정혜영(2011). 개인정보 보호법의 내용과 체계에 관한 분석. 공법학연구, 12(4), pp407~435. 한국비교공법학회.

조혜경(2008). 의료기관의 개인건강정보 보호 실태와 관리방안. 충남대학교 대학원 박사학위논문.

한국인터넷진흥원(2013). 2013 국가정보보호백서.

한국정보보호진흥원(2001). 정보화 역기능 현황과 대응방안.

한국정보보호진흥원(2006). 지식정보사회 의료 패러다임 변화와 정보보안.

한국정보보호진흥원(2009). 주요 국가의 개인정보보호 동향 조사.

한국정보보호진흥원·개인정보분쟁조정위원회(2007). 2007 개인정보분쟁조정사례집.

한국정보화진흥원(2013.10.). OECD 2013년 개정 개인정보보호 가이드라인. 개인정보보호 주간동향 제30호.

함인선(2012). EU개인정보보호법제에 관한 연구. 저스티스, 통권 제133호, pp.5~38.
행정안전부(2008.04.03.). "행정안전부, 중앙·지자체 개인정보보호수준 진단". 행정안전부 보도자료.
행정안전부(2011.12). 개인정보 보호법령 및 지침·고시 해설.
행정안전부(2012.11.9.). "범정부「개인정보보호 합동점검단」출범". 행정안전부 보도자료.
행정안전부·한국인터넷진흥원(2012). 개인정보영향평가수행안내서.
JiPDEC(2013). The PrivacyMark System.
Smith HJ, Milberg SJ, Burke SJ, Information Privacy(1996). Measuring Individuals's Concerns about Organizational Practices. *MIS Quarterly*, 20(2), pp.167-196.

〈사이트〉

국가법령정보센터 사이트. http://www.law.go.kr/. [인용 2013.06.15.].
개인정보보호인증마크제도 사이트. www.eprivacy.or.kr. [인용 2013.10.20.].
개인정보보호 종합지원 포털 중 '안내광장'. http://www.privacy.go.kr/nns/ntc/inf/personalInfo.do. [인용 2013.10.30.].
개인정보보호 종합지원포털사이트 중 '용어사전'. http://www.privacy.go.kr/nns/ntc/wor/WordDicaryListInqire.do. [인용 2013.10.30.].
개인정보 보호 포털사이트. www.i-privacy.kr, [인용 2013.06.10.].
개인정보영향평가 사이트. www.pia.go.kr. [인용 2013.10.20.].
정보보호 및 개인정보보호관리체계 인증 사이트. http://isms.kisa.or.kr/, [인용 2013.10.20.].
의료기관평가인증원 사이트. www.koiha.or.kr. [인용 2013.06.15.].
정보보호 및 개인정보보호관리체계 인증 사이트. http://isms.kisa.or.kr/. [인용 2013.10.20.].

P마크제도 사이트. http://privacymark.jp/. [인용 2013.10.20.].

P마크제도 사이트 중 'P마크 부여사업자 일람'. http://privacymark.jp/certification_info/list/clist.html. [인용 2013.10.20.].

한국브리태니커 온라인. http://preview.britannica.co.kr/bol/topic.asp?article_id=b19j1134b. [인용 2013.10.20.].

한국민족문화대백과. http://terms.naver.com/entry.nhn?docId=547151&cid=1642&categoryId=1642. [인용 2013.10.20.].

한국정보화진흥원 사이트 중 '국제 정보화 지수현황'. http://www.nia.or.kr/Contents/01_data/infostats.asp?BoardID=201112071550550012&order=010501. [인용 2013.06.19.].

〈언론기사〉

경향신문(2004.01.14.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=032&aid=0000049206.

경향신문(2007.10.11.). http://news.khan.co.kr/kh_news/khan_art_view.html?artid=200710111839051&code=910112.

경향신문(2010.02.03.). http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201002031148521&code=940100.

국민일보(2007.10.12.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=143&aid=0000074860.

노컷뉴스(2009.05.19.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=106&oid=079&aid=0002058658.

노컷뉴스(2012.08.20.). www.nocutnews.co.kr/Show.asp?IDX=2230819.

뉴데일리(2012.03.13.). http://www.newdaily.co.kr/news/article.html?no=108916.

뉴시스(2004.07.20.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=003&aid=0000073223.

뉴시스(2004.07.27.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=001&oid=003&aid=0000074457.

동아일보(2001.12.26.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=020&aid=0000105529.

데이터넷(2013.10.07.). http://www.datanet.co.kr/news/articleView.html?idxno=68727.

데일리메디(2011.05.04.). http://www.dailymedi.com/news/view.html?section=1&category=4&no=727103.

데일리메디(2013.07.18.). http://dailymedi.com/news/view.html?section=1&category=4&no=769424.

데일리시큐(2013.01.23.). http://www.dailysecu.com/news_view.php?article_id=3687.

디지털타임스(2013.1.17.). http://www.dt.co.kr/contents.htm?article_no=2013011702011060785002.

머니투데이(2000.11.3.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=008&aid=0000026232.

메디파나(2013.07.10.). http://medipana.com/news/news_viewer.asp?NewsNum=130404&MainKind=A&NewsKind=5&vCount=12&vKind=1.

보안뉴스(2011.09.29.). http://www.boannews.com/media/view.asp?idx=27882&kind=2.

보안뉴스(2013.06.27.). http://www.boannews.com/media/view.asp?idx=36636&kind=1.

부산일보(2006.10.3.). http://www.busanilbo.com/news2000/html/2006/1003/030020061003.1006105606.html.

아시아투데이(2013.10.26.). http://www.asiatoday.co.kr/news/view.asp?seq=884507.

아이뉴스24(2002.05.22.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=031&aid=0000003479.

아주경제(2013.09.23.). http://www.ajunews.com/kor/view.jsp?newsId=20130922000122#.

조선일보(2012.09.28.). http://news.chosun.com/site/data/html_dir/2012/09/28/2012092800063.html.

청년의사(2013.08.07.). http://www.docdocdoc.co.kr/news/newsview.php?newscd=2013080700012.

한국경제(2002.6.17.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=015&aid=0000519209.

한국일보(2012.10.31.). http://news.hankooki.com/lpage/society/201210/h2012103102342221950.htm.

C뉴스041(2012.04.18.). http://cnews041.com/sub_read.html?uid=36164&section=section26.

JTBC TV(2013.10.02.). http://news.jtbc.co.kr/html/132/NB10351132.html.

mbc(2006.10.24.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=115&oid=214&aid=0000021466.

SBS(2004.06.12.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=115&oid=055&aid=0000022954.

YTN(2003.12.04.). http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=129&oid=052&aid=0000020026.

ZDNet Korea(2013.06.20.). http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130620082009&type=det.

〈관련 법·제도 등〉

국가정보화기본법
개인정보 보호법
개인정보 보호법 시행령
정보통신망 이용촉진 및 정보보호 등에 관한 법률
정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령
정부출연연구기관등의 설립·운영 및 육성에 관한 법률
개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45조)
개인정보 보호 관리체계 인증 등에 관한 고시(방송통신위원회고시 제2013-17호)
개인정보의 안전성 확보조치 기준(행정안전부 고시 제2011-43호)
정보보호 관리체계 인증 등에 관한 고시(미래창조과학부 고시 제2013-36호)
표준 개인정보 보호지침(행정안전부 고시 제2011-45호)

간행물회원제 안내

▶ 회원에 대한 특전

- 본 연구원이 발행하는 판매용 보고서는 물론 「보건복지포럼」, 「보건사회연구」도 무료로 받아보실 수 있으며 일반 서점에서 구입할 수 없는 비매용 간행물은 실비로 제공합니다.
- 가입기간 중 회비가 인상되는 경우라도 추가 부담이 없습니다.

▶ 회원종류

- 전체간행물회원 : 120,000원
- 보건분야 간행물회원 : 75,000원
- 사회분야 간행물회원 : 75,000원
- 정기간행물회원 : 35,000원

▶ 가입방법

- 홈페이지(www.kihasa.re.kr) - 발간자료 - 간행물구독안내

▶ 회비납부

- 홈페이지를 통해 신용카드 결제
- 온라인 입금 : 우리은행 019-219956-01-014 (예금주: 한국보건사회연구원)

▶ 문의처

- (122-705) 서울특별시 은평구 진흥로 235 한국보건사회연구원
  간행물 담당자 (Tel: 02-380-8157)

KIHASA 도서 판매처

- 한국경제서적(총판) 737-7498
- 영풍문고(종로점) 399-5600
- Yes24 http://www.yes24.com
- 교보문고(광화문점) 1544-1900
- 서울문고(종로점) 2198-2307
- 알라딘 http://www.aladdin.co.kr

KIHASA Korea Institute for Health and Social Affairs

연구보고서 발간목록

발간번호	보고서명	연구책임자
연구 2013-01	근거중심보건정책에 필요한 연구근거 현황 및 활용	김남순
연구 2013-02	국민건강증진기금사업의 운영현황과 개선방안 연구	김혜련
연구 2013-03	의료서비스산업의 경쟁구조 및 경영효율성에 관한 연구	김대중
연구 2013-04	보건의료서비스 분야의 소비자 위상과 권리	윤강재
연구 2013-05	식품분야 규제정책의 변화와 향후 식품안전 관리강화를 위한 규제합리화	정기혜
연구 2013-06	화장품 및 의약외품에 대한 소비자 중심적 연구	김정선
연구 2013-07	보건의료분야 국가연구개발사업 운영현황 및 개선방안	박은자
연구 2013-08	진료비지출 요인분석 및 거시적 관리방안	신현웅
연구 2013-09	의약품 정책이 의사의 처방에 미친 영향 연구	박실비아
연구 2013-10	한국의 건강불평등 지표와 정책과제	김동진
연구 2013-11	한국 의료의 질 평가와 정책과제 Ⅰ: 한국 의료의 질 보고서 설계	강희정
연구 2013-12	국민연금기금운용 중장기 정책수립	원종욱
연구 2013-13	소득분배 악화의 산업구조적 원인과 대응 방안	강신욱
연구 2013-14	소득계층별 순조세부담의 분포에 관한 연구	남상호
연구 2013-15	저소득층 현금 및 현물서비스 복지지출의 사회경제적 영향분석	김태완
연구 2013-16	기회의 불평등 측정에 관한 연구: 성장배경을 중심으로	김문길
연구 2013-17	2013년 빈곤통계연보	임완섭/노대명
연구 2013-18	고용-복지 연계정책의 국제비교 연구: 한중일의 최근 정책변화를 중심으로	노대명
연구 2013-19	근로 및 사회정책에 대한 국민의식 분석	이현주
연구 2013-20	한국복지패널 연계 질적 연구(3차): 취약계층의 삶을 중심으로	김미곤
연구 2013-21	사회서비스 수요·공급의 지역단위 분석 연구	박세경
연구 2013-22	사회복지영역의 평가제도 분석 및 개선방안	정홍원
연구 2013-23	장애인의 자립생활 지원 방안: 발달장애인을 중심으로	김성희
연구 2013-24	장애인지원서비스의 질과 공급특성 분석 연구	박수지
연구 2013-25	복지재정 DB구축과 지표 분석	박인화
연구 2013-26	중앙과 지방의 사회복지재정 형평화 연구: 재정분담체계 재구조화를 중심으로	고제이
연구 2013-27	사회보장 중장기 재정추계 모형개발을 위한 연구	신화연
연구 2013-28	사회보장 재원조달에서의 세대 간 형평성 제고방안 연구	유근춘
연구 2013-29	의료기관의 개인정보 보호현황과 대책	정영철
연구 2013-30	우리나라 아동빈곤의 특성	정은희
연구 2013-31-01	한중일 인구동향과 국가 인구전략	이삼식
연구 2013-31-02	인구예측모형 국제비교 연구	이삼식
연구 2013-31-03	자녀 양육 지원 정책 평가와 개선 방안	신윤정
연구 2013-31-04	보육서비스 공급 적정성 분석 및 개선방안 연구	김은정
연구 2013-31-05	아동보호체계 연계성 제고방안	김미숙
연구 2013-31-06	여성고용 활성화 방안 연구	여유진
연구 2013-31-07	출산·보육 통계생산 및 관리효율화 연구	도세록

발간번호	보고서명	연구책임자
연구 2013-31-08	가구·가족의 변동과 정책적 대응방안 연구	김유경
연구 2013-31-09	저출산·고령화 대응 인구 자질 향상 방안: 고령 임산부의 출산 실태와 정책 과제	이소영
연구 2013-31-10	저출산고령사회에서의 일차의료기관 모형개발	황나미
연구 2013-31-11	저출산고령사회 동태적분석을 위한 지역 추적조사: 사례지역을 중심으로	오영희
연구 2013-31-12	저출산·고령화 시대의 한국 가족주의에 대한 진단과 정책적 함의	외부위탁
연구 2013-31-13	남북한 통합 시 적정인구 연구	이삼식
연구 2013-31-14	중·노년층의 삶의 질과 정책과제	정경희
연구 2013-31-15	고령화 대응 노인복지서비스 수요전망과 공급체계 개편연구	이윤경
연구 2013-31-16	다층노후소득보장체계 관점에서의 공적연금제도 개편 방안	윤석명
연구 2013-31-17	노인장기요양서비스의 질 관리체계 개선방안	선우덕
연구 2013-31-18	요양병원과 요양시설의 역할정립방안연구: 연계방안을 중심으로	김진수
연구 2013-31-19	효과적 만성질환 관리방안 연구	정영호
연구 2013-31-20	인구고령화가 소비구조 및 산업생산에 미치는 영향 연구	외부위탁
연구 2013-31-21	여성노인의 노후빈곤 현황 및 대응정책	외부위탁
연구 2013-31-22	농촌 노인일자리의 현황과 정책과제	외부위탁
연구 2013-31-23	평생교육관점에서 바라본 노년교육의 현황과 정책과제	이윤경
연구 2013-32-1	지방자치단체의 건강영향평가 및 지식포털운영	서미경
연구 2013-32-2	건강영향평가TWG성과평가 및 건강행태위험요인의 사회경제적 격차감소를 위한 전략평가	최은진
연구 2013-33	아시아국가의 사회정책 비교연구: 건강보장	홍석표
연구 2013-34	취약위기가족 및 다문화가족의 예방맞춤형 복지체계 구축 및 통합사례관리 연구(4년차)	정은희
연구 2013-35	2013년 친서민정책으로서 사회서비스 일자리 확충전략III: 사회서비스산업 -제3섹터-고용창출 연계 모델	이철선
연구 2013-36	2013년 보건복지통계정보시스템 구축 및 운영	오미애
연구 2013-37	인터넷 건강정보 게이트웨이시스템 구축 및 운영: 빅 데이터 활용방안을 중심으로	송태민
연구 2013-38	2013년 사회정신건강 연구센터 운영: 한국사회의 갈등 및 병리현상의 발생현황과 원인분석 연구	이상영
연구 2013-39	2013년 지방자치단체 복지정책 평가센터 운영	김승권
연구 2013-40-1	2013년 한국복지패널 기초분석 보고서	이현주
연구 2013-40-2	2013년 한국복지패널 심층분석 보고서: 신규 표본가구 통합DB(KOWEPS_Combined)을 중심으로	최현수
연구 2013-41	2011년 한국의료패널 기초분석 보고서(II): 만성질환관리, 일반의약품이용, 임산출산, 부가조사	최정수
협동 2013-1	비영리법인 제도의 개선방안에 관한 연구(3년차)	오영호
협동 2013-2	가임기 임신 전 출산건강 관리지원 방안 연구	이상림