보건·복지 Issue & Focus

Korea Institute for Health and Social Affairs

ISSN 2092-7117
제231호(2014-10) 발행일 : 2014. 03. 14

KIHASA 한국보건사회연구원 Korea Institute for Health and Social Affairs

보건복지 개인정보 보호 정책의 발전 방안

국민의 건강과 복지증진을 위해 대량의 민감한 개인정보를 처리하고 있는 보건복지분야의 개인정보보호에 대한 필요성과 중요성이 부각됨

공공 보건복지분야에 대한 정부주도의 주요 개인정보보호 활동으로는 보건복지부 소관법령 개정 및 개인정보보호협의회 운영과 같은 관련 정책 및 제도개선, 개인정보보호 실태조사, 그리고 정부부처 중 유일하게 「개인정보통합관제센터」를 운영하고 있음

향후 보건복지 부문별 맞춤형 교육 및 컨설팅, IT 환경변화에 조응하는 선도적 보건복지 개인정보 보호 기반 기술 강화 및 전문인력 양성, 대국민 개인 보건복지정보 열람 확인 서비스 제공, 보건복지분야 개인정보 보호 인증마크 제도 도입, 보건복지분야 개인정보 보호 컨트롤타워로서의 전담조직 등이 필요함

이야리
정보기술융합센터 초빙연구위원

1. 서론

■ 최근 개인정보는 공공 및 민간 분야에서 다양한 목적으로 폭넓게 이용되는 추세

○ 정보기술(IT)의 발전으로 데이터의 신속·정확한 처리가 용이해지면서, 고객요구에 효율적으로 대응할 수 있는 개인정보에 대한 가치 상승

○ 공공분야에서는 주로 행정 효율성 제고, 맞춤형 민원서비스 제공 등 국민의 편의증진을 목적으로 이용하고 있으며, 민간에서는 고객특성별 타깃마케팅 등 경제적 이익을 극대화 할 수 있는 핵심자원으로 이용

■ 그러나 개인정보 이용이 증가하면서 개인정보의 대규모 유출사고 및 프라이버시 침해사고가 빈번하게 발생하여 개인정보 보호에 대한 관심 급증

○ 최근 연이어 발생하고 있는 카드사, 이동통신업체, 각종 인터넷 사이트의 대규모 개인정보 유출 사고로 인해 개인정보 유출은, 어느 특정영역에만 발생할 수 있는 문제가 아닌 모든 영역에서, 언제든지 발생할 수 있고, 이로 인해 특정 대상 뿐 아니라 모든 국민이 피해대상이 되어 사회 전반적으로 큰 혼란을 초래할 수 있음을 인식하게 되면서 개인정보보호에 대한 중요성 대두

○ 특히 연예인 및 정치인들에 대한 진료기록 유출, 지난해 발생한 대학병원 및 약학정보원의 개인정보 유출 사고 등 민감 개인정보로 분류하는 개인의 질병 및 건강관련 정보 유출은 개인에게 심각한 프라이버시 침해 뿐 아니라 기업차원의 직 · 간접적인 재산상 손해, 정부차원의 신뢰하락 등 많은 피해 예상

■ 국민의 건강과 복지증진을 위해 대량의 민감한 개인정보를 처리하고 있는 보건복지분야의 경우, 유출시 그 피해영향이 더 심각하여 어느 분야보다도 개인정보 보호가 필요

○ 보건복지부 본부, 소속 및 산하기관(이하 "공공 보건복지분야")에서 보유하고 있는 개인정보는 의료정보, 건강정보, 연금정보, 사회복지정보 등 대부분 민감한 개인정보로 구성되어 있으며 그 수는 약 845억건으로[1] 이는 정부기관 전체 보유량 약 1,030억건 대비 82% 차지

○ 그 외 약 59,000여개의 의료기관과 21,000여개의 약국[2], 59,000여개의 사회복지생활시설[3] 등과 같은 보건복지분야 민간기관에서 다루어지고 있는 개인정보도 매우 민감한 정보이나 그 수에 대한 파악조차 안 되어 있는 실정

○ 이렇듯 개인정보의 수 및 내용에 있어 그 어느분야보다도 중요한 보건복지분야에서의 개인정보 유출을 예방하여 개인의 존엄과 가치를 보호하는 선진 보건복지 정보사회구현을 위한 보건복지 개인정보 보호 관리 필요

■ 이에 보건복지분야 개인정보 보호 수준 제고를 위해 현재 공공 보건복지분야에 대한 정부(보건복지부) 주도의 개인정보 보호 활동을 파악해보고 향후 개선방안을 제안

○ 개인정보보호 개념

○ 공공 보건복지분야 주요 개인정보보호 활동 현황

○ 향후 정책제언

1) 개인정보 보호 종합지원 포털(www.privacy.go.kr), 개인정보화일목록[2014.01.27. 인용]
2) 건강보험심사평가원, (http://www.hira.or.kr/rdc_hospsearch.hospsearch.do?method=hospital&pgmid=HIRAA030002000000),[2014.03.04. 인용]
3) 보건복지부(2013), 2013 주요업무 참고자료

2. 개인정보보호 개념

■ 개인정보

○ 개인정보는 국제기구나 국가별 관련 법률 등에서 다양하게 정의하고 있으나, 대체로 개인에 관한 정보로써 직접적으로 개인을 식별할 수 있는 정보 뿐 아니라 간접적으로 개인을 식별할 수 있는 정보까지 포함(표 1 참조)

〈표 1〉 '개인정보' 에 대한 정의

구분		내용
OECD (1980)	프라이버시 가이드라인 제1조	식별된 또는 식별 가능한 개인에 관한 정보
France (2011)	정보처리축적 및 자유에 관한 법 제2조	형식에 관계없이 직접 또는 간접으로 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보
Germany (2009)	연방개인정보보호법 제3조	신원이 확인되었거나 확인 가능한 정보주체의 인적, 물적 환경에 관한 일체의 정보
U.K. (2011)	개인정보보호법 제2조	신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터, 데이터로부터 신원이 확인 가능한 생존 개인과 관련된 데이터
U.S. (1974)	프라이버시보호법 Sec. 552a	개인(미국 시민 또는 법적으로 영주권이 인정된 외국인)에 대한 기록(정부기관에 의해 유지, 수집, 사용 또는 배포되는 개인에 대한 정보의 항목, 수입 또는 집합)

○ 우리나라의 경우 현행 법령 중에서 개인정보를 직접적으로 규정하고 있는 법률은 '개인정보보호법' 과 '정보통신 이용촉진 및 정보보호 등에 관한 법률' 이 있으며, 살아 있는 개인에 관한 정보로서 개인을 직접적으로 식별할 수 있는 정보 뿐 아니라 다른 정보와 쉽게 결합하여 개인을 식별 가능한 정보까지를 포함한다고 규정하고 있어, 국제기구 및 주요 외국의 개인정보 정의와 동일

■ 개인정보 침해

○ 개인정보 침해란 정당하지 않은 절차에 의해 개인정보가 수집 및 이용되고 제3자에게 제공되어 정보주체에게 피해를 입히는 것을 말하며, 개인정보 처리단계별 전 과정에서 발생 가능(그림 1 참조)

[그림 1] 개인정보 처리단계별 개인정보 침해유형

1. 수집	2. 저장 및 관리	3. 이용 및 제공	4. 파기
동의 또는 법적 근거 없이 개인정보 수집	조직 내부 취급자에 의한 개인정보의 유출, 훼손 변경 등	동의 또는 법적 근거 없이 개인정보 무단 제공/공유	수집 및 목적 달성 후 개인정보의 미 파기
동의 또는 법적 근거 없이 정보주체 외로부터 수집	외부인의 불법적 접근에 의한 개인정보 유출 및 훼손 변경	당초 수집 목적을 넘어서는 개인정보의 이용	개인정보 삭제 요구 불응
법정대리인의 동의 없는 개인정보의 수집	사업자의 인식부족, 과실 등으로 인한 개인정보의 공개	타인의 개인정보를 무단으로 이용하는 경우	
서비스 이용과 관련 없는 과도한 개인정보의 수집	기술적, 관리적 조치미비로 인한 개인정보의 유출		
해킹 등 불법 수단에 의한 개인정보의 수집 등	고객의 개인정보클레임에 대한 불응 또는 미 조치 등		

■ 개인정보 보호원칙

○ 개인정보 보호원칙의 의의

– 개인정보 보호원칙은 「개인정보 보호법」 제3조에 정의되고 있으며, 선언적 규범으로써 그 자체가 개인정보처리자를 직접적으로 구속하지는 않지만 행동 지침을 제시해 주고, 정책담당자에게는 정책수립 및 법 집행의 기준을 제시해 주며, 사법부에 대해서는 법 해석의 기초를 제시해 줌과 동시에 입법의 공백을 막아주는 역할

○ 국내외 개인정보 보호원칙 비교

– 개인정보 보호원칙은 우리나라의 개인정보 보호법, OECD 프라이버시 가이드라인(8원칙), EU 개인정보 보호지침 등이 있음

– 우리나라 「개인정보 보호법」은 적용 대상을 공공기관에서 민간으로 확대하고 개인정보 생명주기(수집, 활용 및 파기)별 처리절차에 대한 규율 포함

– OECD 프라이버시 가이드라인은 개인정보 수집 및 관리에 관한 내용을 중심으로 세계 각국의 개인정보 관련 법률과 지침개발을 위한 기초자료로 활용

– EU 개인정보 보호지침은 EU회원국들을 대상으로 한 EU 차원에서의 최초의 입법형식으로 정보처리자의 의무, 정보주체의 권리, 제3국으로의 정보이전 금지, 독립기구 설치에 관한 내용으로 구성

〈표 2〉 국내외 개인정보 보호원칙 비교

우리나라의 개인정보 보호원칙[1]	OECD 프라이버시 가이드라인의 보호원칙[2]	EU 개인정보 보호지침의 보호원칙[3]
– 목적에 필요한 최소정보의 수집(제1항) – 사생활 침해를 최소화하는 방법으로 처리(제6항) – 익명처리의 원칙(제7항)	– 수집제한의 원칙	– 공정하고 적법한 개인정보 처리
– 처리목적 내에서 정확성, 완전성, 최신성 보장(제3항)	– 정보내용 정확성의 원칙	– 개인정보 정확성과 최신성 확보
– 처리목적의 명확화(제1항)	– 목적 명확성의 원칙	– 정보처리 목적 명시
– 목적 범위 내에서 적법하게 처리, 목적의 활용 금지(제2항)	– 이용제한의 원칙	– 정보처리 목적과의 적절성, 관련성, 비례성 유지
– 권리침해 가능성 등을 고려하여 안전하게 관리(제4항)	– 안전성 확보의 원칙	– 기술적, 조직적 보안조치 확보
– 개인정보 처리방침 등 공개(제5항)	– 공개의 원칙	
– 열람청구권 등 정보주체의 권리보장(제5항)	– 정보주체 참여의 원칙	– 정보처리의 전반적인 사항에 대하여 통지받을 권리 – 정보처리에 대해 협의할 권리 – 자신의 개인정보에 대해 수정을 요구할 권리 – 특정 상황에서의 개인정보 처리에 대해 반대할 권리
– 개인정보처리자의 책임준수, 신뢰확보 노력(제8항)	– 책임의 원칙	– 감독기구에 정보처리에 대하여 고지

주: 1) 개인정보 보호법 제3조(개인정보 보호 원칙)
2) OECD 홈페이지(http://www.oecd.org), "the Protection of Privacy and Trans boarder Flows of Personal Data" [2014.03.04. 인용]
3) 전은정외(2012), 유럽의 개인정보보호 법 · 제도 동향, 정보보호학회지 제22권 제2호, pp58~72.

3. 공공 보건복지분야 주요 개인정보 보호 활동

■ 개인정보 보호 정책 및 제도 개선

○보건복지부 소관법령 개정

– 「개인정보 보호법」 시행에 따라 민감정보 및 고유식별정보 수집에 대한 법적 근거 마련을 위해 보건복지부 소관 법령 개정

– '주민등록번호 수집 · 이용 최소화 종합대책(2012.04)'에 따라 보건복지부 소관법률 및 하위법령을 대상으로 개인정보 수집 및 처리에 관하여 법령개정 추진

○유관기관 협업체계 구축

– 보건복지부는 소관분야의 개인정보 보호업무에 대한 원활한 정책결정을 위하여 보건복지부 개인정보 보호책임자(기획조정실장)를 위원장으로 하고 본부내 분야별 책임관과 소속 및 산하기관의 개인정보 보호책임자를 위원으로 하는 '개인정보보호협의회'를 정기적(반기별 1회, 연간 2회)으로 운영

– 개인정보 보호와 관련된 주요 정책 및 현안과제 등에 대한 구체적인 추진방안 및 해결책 등에 대한 정보공유와 우수사례 등을 전파하기 위한 목적으로 보건복지부 정보화담당관을 위원장으로 하고 본부내 분야별 개인정보보호 실무담당자와 소속 및 산하기관의 개인정보보호 실무담당부서장을 위원으로 하는 '개인정보보호 실무협의회'를 수시(연간 3~4회)로 운영

■ 개인정보보호 관리체계 구축 및 운영

○개인정보 보호 실태조사

– 2008년부터 보건복지부는 본부, 소속 및 산하기관의 개인정보 보호 관리수준을 점검함으로써 개인정보 보호를 위한 의무 준수사항 이행 독려 및 개인정보 보호 관리수준 향상 도모

– 개인정보 보유 규모 및 중요성, 그리고 '국가정보보안 기본지침' 제29조의 전자정보 보호등급 분류 등을 기준으로 대상기관을 가급(매년 점검)과 나급(3년마다 점검)으로 분류하여 정기적으로 실시(표 3 참조)

〈표 3〉 보건복지 개인정보 보호 실태조사 점검대상기관 현황('13년 현재)

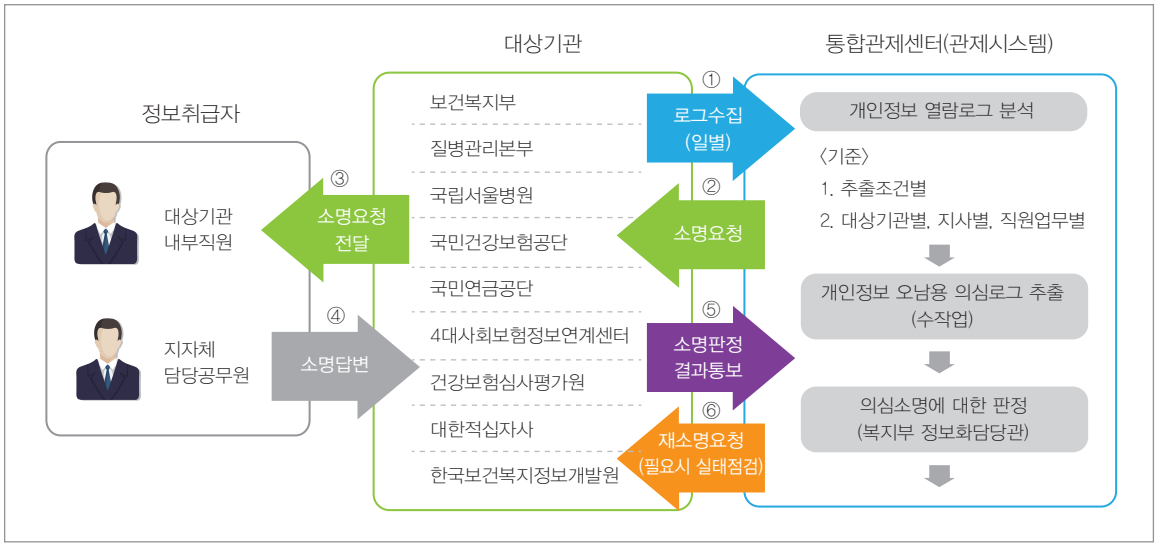
유형	내용
'가'급 기관 (매년 점검)	병관리본부, 국민건강보험공단, 국민연금공단, 건강보험심사평가원, 보건복지정보개발원, 대한적십자사, 국립암센터, 국립중앙의료원
'나'급 기관 (3년마다 점검)	국립부곡병원, 국립소록도병원, 국립재활원, 국립마산병원, 한국사회복지협의회, 한국보건의료연구원, 한국보육진흥원, 한국보건복지인력개발원, 한국의료분쟁조정중재원

– 주요 점검항목은 개인정보보호 관리체계 구축, 보호대책 수립 및 시행, 침해사고 대책, 개인정보처리, 안전성 확보조치, PC내 개인정보보호 관리, 전년도 지적사항 이행여부 등 대상기관의 개인정보보호 관리 수준을 객관적으로 진단할 수 있는 평가지표를 마련하여 점검

○ 보건복지개인정보통합관제센터 운영

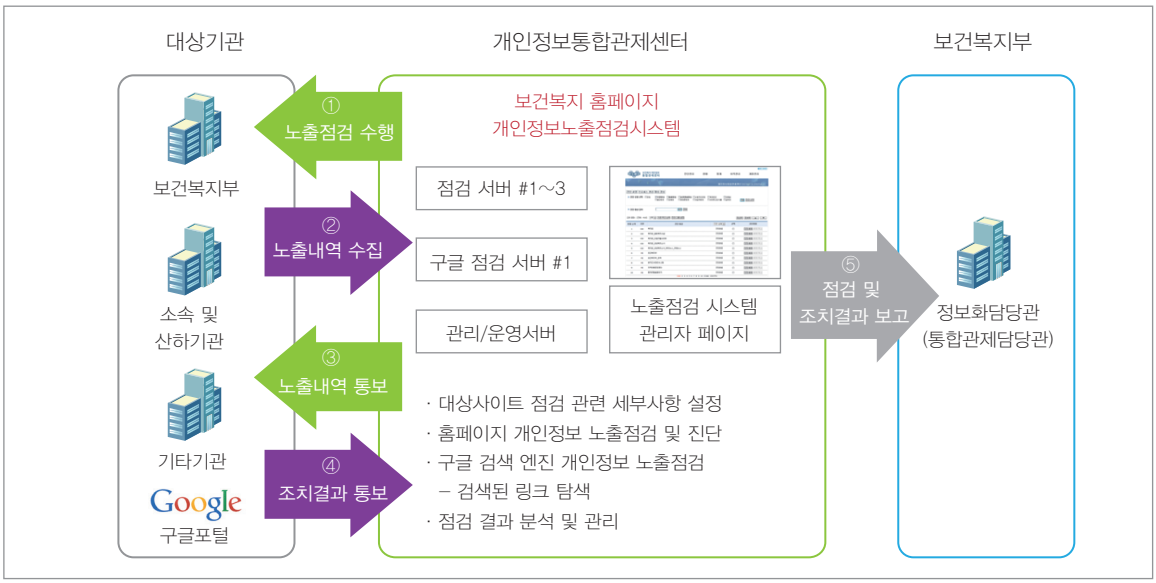
– 개인정보를 다수 취급하는 보건복지부 본부, 소속 및 산하기관의 주요 정보시스템을 대상으로 2010년부터 개인정보 유출 및 오남용 방지를 위한 '보건복지 개인정보통합관제시스템'을 구축 · 운영하여 관제활동을 실시하고 있으며(그림 2 참조), 2012년부터는 총리실 산하 국책연구기관인 '한국보건사회연구원'에서 이를 위한 「보건복지개인정보통합관제센터」를 위탁운영

[그림 2] 보건복지 개인정보통합관제활동 업무흐름도



– 또한 「보건복지개인정보통합관제센터」에서는 2013년부터 '홈페이지 개인정보 노출점검시스템'을 운영하여, 대국민 서비스를 목적으로 운영하는 보건복지부 본부, 소속 및 산하기관, 유관기관 등의 홈페이지를 대상으로 주민등록번호 등 개인정보를 주기적으로 검색하여 홈페이지 개인정보 노출에 대한 선제적 대응 및 피해 최소화를 위한 노력 경주(그림 3 참조)

[그림 3] 보건복지 홈페이지 개인정보 노출점검활동 업무흐름도



■ 개인정보보호 교육 · 홍보

○ 차별화된 개인정보보호 교육

– 보건복지부 본부 및 소속기관, 산하기관, 국 · 공립병원을 대상으로 개인정보 보호 연간 교육계획을 수립하여 교육대상별(관리자, 담당자, 취급자 및 일반직원, 신규입사자 등), 교육방법별(온라인 교육, 집합교육), 교육내용별 교육과정을 세분화하여 교육 추진

○보건복지 영역별 가이드라인 개발

– 의료기관, 약국, 사회복지시설 등 보건복지분야 기관에서 개인정보를 처리할 때 지켜야 할 기준과 원칙에 대한 영역별 개인정보보호 가이드라인을 개발하여 보급

4. 향후 정책제언

■ 보건복지 부문별 맞춤형 교육 및 컨설팅

○개인정보통합관제 활동 및 개인정보 실태점검 등을 통해 대상기관별 미흡 혹은 취약 부분을 파악하여 개인정보 보호 관리수준 향상을 위한 맞춤형 교육 및 컨설팅 제공 필요

○뿐만 아니라 의료기관, 약국, 사회복지시설 등과 같은 민간기관을 대상으로 하여 개인정보 보호 관리실태를 파악하고 이를 기반으로 한 맞춤형 교육 및 컨설팅 제공 필요

■ IT환경 변화에 조응하는 선도적 보건복지 개인정보보호 기반 기술 강화 및 전문인력 양성

○ 공공 빅 데이터 구축 등과 같은 IT 산업기술의 발달은 한편 개인정보 유출에 대한 우려를 증폭시키고 있는 바, 이에 상응하는 개인정보 보호 전문기술 및 전문인력 양성 필요

■ 대국민 개인 보건복지정보 열람 확인 서비스 제공

○ 보건복지 소속 및 산하기관의 개인정보처리시스템에서 처리되고 있는 정보주체 및 개인정보취급자에 대한 개인정보 열람기록 확인 서비스를 제공하여 국민의 개인정보 처리에 대한 알권리 충족 필요

■ 보건복지분야 개인정보보호 인증마크 제도 도입

○ 의료분야와 같이 민감한 개인정보를 취급하는 업종 등에 한하여 국내외 기준을 참고하여 업종별 세부기준을 마련하고 기관의 자발적 인증마크 취득에 대한 다양한 인센티브를 마련하여 개인정보보호 자율적 활동에 대한 장려 정책 필요

■ 보건복지분야 개인정보 보호 컨트롤타워로서의 전담조직 필요

○ 현재는 보건복지 공공분야만을 대상으로 정부주도의 개인정보 보호활동이 이루어지고 있는 바, 향후 의료기관, 약국, 사회복지시설 등 민간 보건복지분야까지 확대된 개인정보 보호 활동 필요

○ 이에 보건복지분야 특성에 맞는 개인정보 보호활동을 적극적이고 포괄적으로 펼칠 전담조직 필요

집필자 | 이야리 (정보기술융합센터 초빙연구위원)　문의 | 02-380-1659

발행인 | 최병호　**발행처** | 한국보건사회연구원
(122-705)서울특별시 은평구 진흥로 235 | TEL 02)380-8000 | FAX 02)352-9129 | http://www.kihasa.re.kr
한국보건사회연구원 홈페이지의 발간자료에서 온라인으로도 이용하실 수 있습니다. http://www.kihasa.re.kr/html/jsp/publication/periodical/focus/list.jsp