

보건의료에서 빅데이터 활용의 법과 정책

박 형 옥 | 단국대학교 의과대학 인문사회학연구소

Policy and law of big data use in health care

Hyoung Wook Park, MD

Department of Social Medicine, Dankook University College of Medicine, Cheonan, Korea

According to Article 17 of the Korean Constitution, the privacy of no citizen shall be infringed. There have been considerable advances in the fields of computers and communications technology in the late 20th century. However, processing large amounts of personal information has caused many problems. In Korea, incidents of personal information leakage have been occurring frequently. To solve these problems, the Personal Information Protection Act was enacted in 2011. The most significant feature of this Act is that it applies not only to public institutions, but also to corporate bodies, organizations, and individuals who manage personal information. However, the Act does not allow the management of personal information for public purposes such as public health. Recently, the European Parliament has adopted a legislative resolution on the proposed European Union General Protection Regulation. This regulation allows the management of personal information for public health, reflecting the opinions of European public health experts. According to Article 81 of the proposed regulation, processing of personal data concerning health is permitted for the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment, or the management of health-care services. It is also permitted for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety for medicinal products or medical devices and reasons of public interest in areas such as social protection, in order to ensure the quality and cost-effectiveness of the health insurance system and the provision of health services. The proposed regulation is an example of the balance of privacy and public interest in the management of personal information. Although the management of personal information is allowed in the public interest without the consent of the subject of the information, all measures should be taken for privacy protection. It is time for Korea to take legislative steps for the management of personal health information for public health under conditions of strict privacy protection measures.

Key Words: Personal health information; Privacy; Consent; Public interest

서론

헌법 제17조는 ‘모든 국민은 사생활의 비밀과 자유를 침해하지 아니한다’고 규정하여 프라이버시권을 헌법상의 기

본권으로 인정하고 있다[1]. 특히 20세기 후반 컴퓨터와 통신기술이 비약적으로 발전함에 따라 정보의 수집과 전파는 더욱 용이해졌으며 개인정보의 대량적 처리는 많은 문제점을 야기하고 있다[2]. 특히 개인정보의 의미에 대하여 둔감한 우리 사회에서 개인정보 보호를 위해 앞으로도 많은 노력을 기울여야 함은 주지의 사실이다.

그러나 개인정보의 활용이 당사자의 동의에 절대적으로 의존하는 것은 아니다. 과거 공공기관의 개인정보보호에 관한 법률은 물론 현재의 개인정보보호법 역시 범죄의 수사과 공소의 제기 및 유지에 필요한 경우나 법원의 재판업무수행을 위하여 필요한 경우 등 일정한 요건 아래 개인정보의 공

Received: April 1, 2014 Accepted: April 15, 2014

Corresponding author: Hyoung Wook Park
E-mail: hywopark@gmail.com

© Korean Medical Association

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

개와 이용이 허용된다. 이처럼 공익과 사익을 비교형량하여 정보의 활용 여부를 결정해야 한다는 원칙은 건강정보라고 해도 마찬가지이다.

이 때문에 유럽연합(European Union, EU)은 1995년 개인정보보호지침에서 예방의학, 의료서비스 관리 목적으로 직업적 비밀유지 의무가 있는 보건전문가 등이 자료를 처리하는 경우 정보주체의 명시적 동의가 없이도 진료정보를 사용할 수 있다는 예외적 조항을 규정해 놓았다. 그러나 이 예외적 조항을 회원국에 강제 적용하는 것은 아니었기 때문에 일부 국가만이 공공이익을 위한 개인정보의 이용을 허용해 왔다. 예를 들어, 스칸디나비아 국가들은 등록된 자료의 자료연계를 허용하고 보건의료의 개선을 위한 전략을 마련할 수 있도록 정책결정자뿐 아니라 연구자들에게도 위 자료의 이용을 허용해 왔다[3].

우리나라에서는 최근까지 개인정보유출 사건이 빈번하게 발생해 왔다. 이로 인해 개인정보보호에 큰 결함이 있다는 견해가 지배적이었고 개선이 필요하다는 지적이 잇따랐다. 개인정보보호법이 제정된 2011년은 개인정보보호 2.0 시대의 개막으로 널리 받아들여졌다.

그러나 불과 1년 후 빅데이터의 활용에 대한 장밋빛 예측이 넘쳐 나기 시작했다. 2012년 정부가 관계부처합동으로 빅데이터마스터 플랜을 내놓은 후 국민건강보험공단과 건강보험심사평가원은 경쟁적으로 빅데이터 활용을 위한 계획을 쏟아내기 시작했다. 우리 사회의 화두가 갑자기 빅브라더에서 빅데이터로 바뀐 것이다.

그러나 이러한 계획들이 건강정보의 특수성을 제대로 검토했는지는 의문이다. 건강정보의 특수성을 고려하지 않고 시행된 개인정보보호법이 의료현장과 의학연구에서 여러 가지 장애와 혼란을 초래한 것처럼 사회흐름에 편승하여 깊이 있는 검토 없이 전혀 다른 맥락의 정책이 추진된다면 머지않아 또 다른 장벽에 부딪칠 것이다.

가장 내밀한 건강정보는 다른 어떤 정보보다 더 강력하게 보호해야 하는 당위성을 갖고 있지만 때로는 공적 목적을 위해 적극적으로 활용할 수밖에 없는 상황도 존재한다. 얼핏 상충되어 보이는 이 두 가지 정책 목표를 정확히 이해하고 보건의료분야에서 빅데이터 활용의 법과 정책을 모색해야 할 것이다.

아래에서는 1) 최근 전면 시행된 개인정보보호법이 공중보건과 같은 공익적 목적을 위한 개인정보 사용에 대하여 어떻게 규정하고 있는지를 살펴보고, 2) 1995년 EU의 개인정보보호지침과 2014년 EU 의회를 통과한 정보보호기본규칙안이 내용을 검토한 후, 3) 우리나라에서 공중보건을 위한 개인정보의 사용에 관한 입법적 조치의 필요성에 대하여 논의하고자 한다.

개인정보보호법 제정과 보건의료

개인정보보호법은 2011년 3월 국회를 통과하여 2011년 9월부터 시행되고 있다. 과거 17대 국회에서 민노당 노회찬 의원, 열린우리당 이은영 의원, 한나라당 이혜훈 의원이 개인정보보호법안을 발의하였으나 임기만료로 자동폐기된 바 있다. 이후 18대 국회에서 2008년 10월 한나라당 이혜훈 의원과 민주당 변재일 의원이 개인정보보호법안을 발의하고 2008년 11월 정부안이 발의되어 오랜 논의 끝에 행정안전위원회 대안으로 상임위를 통과하고 2011년 3월 국회를 통과하게 된 것이다. 이 법의 제정으로 기존의 ‘공공기관의 개인정보보호에 관한 법률’은 폐지되었고, ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’ 중 준용사업자, 분쟁조정위원회 조항 등은 삭제되어 개인정보보호법에 흡수되었다.

개인정보보호법의 가장 큰 특징은 적용대상이 공공기관에 한정되지 않고 개인정보파일을 운용하기 위해 개인정보를 처리하는 자는 모두 적용 대상이 된다는 점이다. 따라서 규율대상이 오프라인 사업자, 의료기관, 협회·동창회 등 비영리단체, 국회·법원·헌법재판소·중앙선거위원회 등으로 확대되었다. 이 외에도 개인정보보호법은 ① 개인정보 수집·이용·파기 단계별 공통기준의 정립, ② 개인정보 암호화, 민감정보·고유식별정보 처리 등 안전성 조치의 강화, ③ 개인정보 열람·정정·삭제권, 집단분쟁, 단체소송 등 피해구제 강화, ④ 개인정보보호위원회 설치 등 추진체계 확립, ⑤ 벌칙강화로 개인정보유출에 대한 대응 강화 등의 특징을 갖고 있다[4].

반면, 개인정보의 범위 자체는 과거 공공기관의 개인정보

보호에 관한 법률과 동일하게 규정되어 있다. 따라서 ‘개인 정보’란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다[5]. 또한 ‘개인정보의 이용 및 제공 제한’에 대한 규정은 사실상 과거 공공기관의 개인정보보호에 관한 법률의 내용과 동일하다. 따라서 개인정보처리자는 다음 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다[6]. ① 정보주체로부터 별도의 동의를 받은 경우, ② 다른 법률에 특별한 규정이 있는 경우, ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, ④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우, ⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우, ⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우, ⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우, ⑧ 법원의 재판업무 수행을 위하여 필요한 경우, ⑨ 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우이다.

의료기관은 의료법에 따라 진료기록부, 진단서, 처방전 등에 주민등록번호 등 개인정보를 사용하도록 하고 있으며 일정기간(환자정보 5년, 진료기록 10년) 보관하도록 의무화하고 있다[7]. 따라서 이 경우는 개인정보보호법 제18조 제2항 제2호의 ‘다른 법률에 특별한 규정이 있는 경우’가 적용되므로 진료의 예약, 진단, 진단결과 통보, 진료비 청구, 증명서 발급, 진단결과 통보를 위한 연락처 정보까지는 동의 없이 수집 가능하다. 그러나 의료기관에서 진료정보, 학술정보, 병원소식 등의 안내 및 환자의 의견수렴을 위해 휴대전화 문자, 이메일 등을 통해 추가 서비스를 제공하는 경우에는 이

에 필요한 개인정보에 대하여 동의를 받아야 한다. 마찬가지로 의료기관에서 운영하는 홈페이지를 통해 진료정보, 학술정보, 병원소식 등의 안내 및 환자의 의견수렴을 목적으로 회원가입을 받는 경우 역시 동의 절차가 필요하다[8].

‘학술연구를 위한 개인정보의 이용 및 제공’ 역시 과거 공공기관의 개인정보보호에 관한 법률과 동일하게 규정되어 있다. 즉 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우에는 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우에만 가능하다. 따라서 개인정보보호법은 다른 법률에 특별한 규정이 없는 경우 자료 연계를 통한 활용이나 학술연구는 허용하지 않고 있다고 해석된다.

유럽연합의 개인정보보호와 보건의료

1. 2005년 유럽연합 개인정보보호지침과 보건의료

EU 기본권헌장(Charter of Fundamental Rights)은 제8조에서 개인정보보호의 권리를 명시하고 있으며 EU 기능조약(Treaty on the Functioning of the European Union)은 제16조에서 개인정보 보호의 권리를 규정하고 있다. 이에 따라 2005년 EU는 개인정보의 처리와 자유로운 이동시의 개인의 보호에 관한 1995년 10월 24일 유럽의회와 EU이사회 지침(95/46/EC)을 제정하였다[9]. 이것을 통상 ‘EU Data Protection Directive (EU DPD)’라 한다. EU 개인정보보호지침은 개인의 정보보호와 관련하여 가장 엄격한 법규범의 하나로 인정되고 있다.

EU DPD 제8조 제1항에 따르면 회원국들은 민족 또는 인종적 기원, 정치적 의견, 종교 또는 철학적 믿음, 노동조합 회원자격을 드러내는 개인정보의 처리 및 건강 또는 성생활에 관한 자료의 처리를 금지해야 한다. 그러나 EU DPD는 개인정보를 불가침의 권리로 주장하고 있는 것은 아니며 이 익형량을 통하여 여러 가지 예외를 인정하고 있다. 대표적인 경우가 당사자의 명시적 동의가 있는 경우에는 당연히 그러한 자료의 처리가 가능하다[9].

또한 EU DPD 제8조 제3항은 ‘예방 의학, 의학적 진단, 돌봄과 진료, 의료서비스 관리 목적으로 자료의 처리가 필요하

고 국내법 또는 담당 기관의 규정에 따라 직업적 비밀유지의무가 있는 보건의로 전문가(health professional)나 이와 동등한 비밀 유지 의무가 있는 다른 사람에 의하여 위 자료가 처리되는 경우에 제1항은 적용되어서는 아니 된다'고 규정하고 있다[9].

그리고 EU DPD 제8조 제4항은 '회원국들은 실질적인 공공이익이 존재하는 경우, 적절한 보호 장치의 제공을 조건으로, 국내법 또는 감독 기관의 결정에 의하여 제8조 제2항에서 정한 예외 사유 외에 추가하여 동의 적용 면제 사유를 정할 수 있다'고 규정하고 있다[9]. 여기서 공공이익이라 함은 공중보건과 사회 보호(특히 의료보험제도에서 급부와 서비스의 청구 관련 절차의 질과 비용-효과성을 보장하기 위하여), 과학적 연구와 정부 통계 등을 의미한다.

이 규정에 따르면 EU 회원국에 있어 특별하고 적절한 보호 장치를 마련한다면 보건의로 연구를 위하여 개인정보를 처리함에 있어 개인의 동의가 필수적으로 요구되는 것은 아니다. 예를 들어, 스칸디나비아 국가들은 등록된 자료의 자료 연계를 허용하고 보건의료의 개선을 위한 전략을 찾아낼 수 있도록 정책결정자뿐 아니라 연구자들에게도 위 자료의 이용을 허용해 왔다. 그러나 EU DPD는 회원국에 예외에 대한 여지를 허용하고 있을 뿐 예외적 조치의 시행을 강제하는 것은 아니었다.

따라서 유럽의 많은 나라들은 이에 대하여 소극적으로 대처하였다. 스칸디나비아 국가들과 영국, 프랑스 등 일부 국가들만 중요한 공공이익을 위하여 민감 정보의 처리를 정당화하는 법률을 마련하였을 뿐이다. 그 결과 공중보건 또는 보건의료 연구와 같은 영역에서 EU DPD를 적용함에 있어 회원국의 정책이 상이하여 국가 간 비교 등에 있어 상당한 문제가 야기된다는 비판의 목소리가 높아졌다. 이에 따라 EU 자문기구에서 특별조사가 이루어졌으며 이후 EU 집행위원회는 회원국이 EU DPD를 부정확하게 적용해 왔다는 사실을 인정하게 되었다[3].

2. 2010년 유럽연합 개인정보보호지침 개정 논의

2010년 11월 4일 EU는 1995년 EU DPD를 개정하기 위하여 'EU에서 개인정보보호를 위한 포괄적 접근(A

comprehensive approach on personal data protection in the European Union)'을 발표하고 관련 당사자들의 의견을 조회하였다[10]. EU에서 이런 논의를 시작한 이유는 디지털 환경이 가속되면서 개인정보보호를 강화하면서도 개인정보의 자유로운 이전을 보장할 필요성이 있었기 때문이다. EU가 제시한 지침의 개정 방향은 다음과 같다. 첫째, 개인정보의 수집과 사용이 최소한의 필요에 따르도록 개인의 권리를 강화한다. 둘째, 기업의 행정적 부담을 경감하기 위하여 EU 단일시장 안에서 개인정보의 원활하고 자유로운 이전을 도모한다. 셋째, 개인정보가 수사 및 형사 절차에서도 보호될 수 있도록 이들 분야에서의 개인정보보호에 관한 규범을 개선한다[11].

그러나 공중보건 연구자들은 제안된 문건을 검토한 후 그 내용이 공중보건 영역에서 자료이용 제한을 야기하는 핵심적인 사항들을 해결하지 못하고 있다는 결론에 도달하였다. 이에 따라 2010년 공중보건 연구자들이 모여 워크숍(EUPHEX, European Public Health Experts Workshop on Privacy Protection)을 진행하고 입장을 정리하여 EU 집행위원회에 공식적인 의견을 전달하였다[3]. 이 문건에서 유럽 공중보건 연구자들은 개인정보보호에 대한 EU의 목표에 대하여 전적으로 동의하나 개정안이 공중보건을 위하여 개인정보를 사용하는 것에 대한 실효성 있는 조항을 포함하지 않는다면 EU가 희망하는 '포괄적 접근'을 실현할 수 없다는 견해를 밝혔다. 즉 개인의 프라이버시권에 대한 보호는 건강권의 보호와 같이 사회에 도움을 줄 수 있는 다른 권리들과 균형을 이루는 것이 무엇보다 중요하다는 것이다. 유럽 공중보건 연구자들은 구체적으로 다음의 사항을 지적하였다.

첫째, 개인정보를 보호하는 입법에서 반드시 공중보건을 위한 정보 이용을 보장해야 하는 이유는 다음과 같다. 개인정보에 대한 직접적인 접근이 허용되지 않으면 공중보건에 대한 정확한 통계적 분석은 불가능하다. 프라이버시 보호를 충분히 보호할 수 있는 조건 하에 다양한 자료원 사이의 자료연계가 분명히 허용되고 적절하게 관리되는 경우에만 가장 정확한 결과를 산출할 수 있다. 공중보건 목적으로 개인정보를 처리하는 것을 명백하게 허용하지 않는 건강정보 체계는 합당한 관리를 보장할 수 없다.

둘째, EU DPD 개정안은 구체적으로 다음과 같은 내용들을 담고 있어야 한다. 우선 개정안은 공중보건을 위하여 개인식별 정보를 합법적으로 처리하는 것을 허용해야 한다. 즉 개인식별 정보를 안전하게 처리하는 조건을 규정한다는 전제 하에 환자의 동의 없이 공중보건을 위하여 특정 국가나 지역별로 개인식별정보를 합법적으로 처리하는 것을 허용하는 명시적인 조항이 개정안에 포함되어야 한다.

또한 개정안은 데이터베이스 접근에 대한 투명성을 명확히 규정해야 한다. 다시 말해 개정안은 공중보건 데이터베이스를 이용할 수 있다는 것을 투명하게 명시하고 담당 기관의 승인을 얻을 수 있는 조건을 공개하도록 회원국에 의무를 부과해야 한다. 그리고 개정안은 회원국이 공중보건 데이터베이스의 이용을 위한 공통 사건을 구축하는 구상을 포함해야 한다.

그리고 개정안은 공중보건을 위하여 회원국 간에 건강정보의 합법적인 이동에 대한 조건을 명시하도록 회원국에 의무를 부과하고 유럽 전역에서 EU DPD의 균일한 실행과 그것이 공중보건에 미치는 영향을 EU 집행위원회가 모니터링하도록 책임을 부과해야 한다.

3. 2014년 유럽연합 의회의 정보보호기본규칙안 통과

1) 논의 경과

EU 집행위원회는 2010년 제안된 안에 대한 의견을 수렴한 후 2012년 1월 25일 다시 규정안을 발표하였다[12]. 이 정보보호기본규칙안(General Data Protection Regulation)은 개인정보의 처리와 자유로운 이동에 있어 개인의 보호에 관한 EU 의회와 각료회의의 규칙안(Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data)이라는 긴 이름을 달고서 단순한 '지침(directive)'에서 '규칙(regulation)'으로 강화되었다. 규칙안의 제3장 제17조에서는 잊혀질 권리와 삭제권(right to be forgotten and to erase)을 규정하는 등 개인정보에 대한 정보주체의 권한을 강화하였다.

그러나 정보보호규칙안은 공중보건 목적을 위한 개인정

보의 처리를 다른 학술연구 목적을 위한 개인정보 처리와 구분하여 규정하고 있다는 점에서 유럽 공중보건 연구자들의 제안을 상당 부분 반영하고 있다.

이후 2012년 EU 집행위원회를 통과한 정보보호규칙안은 2013년 일부 수정되어 EU 자유정의위원회(The European Parliament's Committee on Civil Liberties, Justice and Home Affairs)를 통과하였다. 그리고 이 정보보호규칙안은 2014년 3월 12일 찬성 621, 반대 10, 기권 22의 압도적인 표차로 EU 의회를 통과하였다[13,14]. 요컨대 EU 의회는 EU 집행위원회가 만든 정보보호규칙안의 기본구조와 근본원리에 대하여 압도적인 지지를 표한 것이다. EU 의회를 통과한 정보보호규칙안은 앞으로 EU 각료이사회에서 채택된 후 공동결정의 형식으로 최종적인 입법과정을 거치게 된다.

정보보호규칙안이 법으로 확립되면 경제적인 측면에서 다음 세 가지 의미를 갖게 된다. 우선, 각 나라마다 상이한 법령이 존재하는 현재의 상황과 달리 이제 EU에서는 정보보호와 관련하여 단 하나의 법만이 존재하게 된다(one continent, one law). 이러한 변화의 경제적 효과는 매년 230억 불에 해당할 것으로 추정된다. 또한 기업에게는 28개의 다양한 규제기관이 아니라 단일한 하나의 규제기관을 대상으로 업무를 처리하면 된다(one-stop-shop). 마지막으로 EU 내에서는 기업이 어디에 소재하던 동일한 규정의 적용을 받게 된다(the same rules for all companies: regardless of their establishment).

또한 정보보호규칙안이 법으로 확립되면 EU 시민의 정보보호라는 측면에서 다음과 같은 변화가 뒤따르게 된다. 첫째, EU 시민은 자신의 정보가 더 이상 처리되는 것을 원하지 않고 정보처리자의 정보보유에 합법적 근거가 없다면 그 정보를 삭제시킬 수 있다(a right to be forgotten). 물론 과거의 사건을 삭제하거나 언론의 자유를 제한할 수는 없다. 둘째, 정보 이동권을 통하여 자신의 개인정보를 서비스 제공자 사이에서 이전시키는 것이 용이해질 것이다(easier access to your own data). 마지막으로 정보처리에 대한 동의는 명시적인 방법을 사용해야 한다(putting you in control).

2) 개인 건강정보의 처리

정보보호규칙안 제9조 제1항은 인종, 정치적 견해, 종교

혹은 철학적 신념, 성적 기호 또는 성적 정체성, 노동조합 가입과 활동, 유전적 혹은 생체인식 자료, 건강과 성생활에 대한 정보 등 개인정보의 처리는 금지된다는 원칙을 규정한 후 제9조 제2항에서 적용 예외 사항을 규정하고 있다. 그 중 (h) 목은 보건의료를 위한 목적으로 제81조에 규정된 조건 아래에서 건강정보의 처리를 허용하고, (i)목은 역사, 통계, 혹은 과학을 위한 목적으로 제83조에 규정된 조건 아래에서 관련된 정보의 처리를 허용하고 있다[14].

정보보호규칙안 제81조에 의하면 개인 건강정보의 처리는 EU 또는 회원국의 법에 의거해야 하며 그 법은 정보주체의 정당한 이해와 기본권 보호에 합당하며 일관성 있는, 적합한 수단을 규정해야 한다. 또한 그 보호수단은 필수적인 것을 포함하고 비례원칙에 부합하고 정보주체가 예견할 수 있는 정도가 되어야 한다. 이러한 요건 하에서 다음 목적을 위해 개인 건강정보의 처리가 가능하다[14].

우선 예방의학, 산업의학, 의학진단, 치료나 요양의 제공, 의료서비스의 관리를 목적으로 해야 하며 직업적 비밀유지 의무가 있는 보건의료 전문가들 또는 회원국의 법 또는 국가 기구의 규정에 의해 상당한 비밀유지 의무가 있는 사람들이 관련 정보를 처리하는 경우 개인 건강정보의 처리가 가능하다. 또한 의약품, 의료기기에 대한 높은 수준의 질과 안전 보장, 국경을 넘는 중대한 건강 문제로부터의 보호 등 공중보건 영역에서 공공이익을 위한 경우에도 개인 건강정보의 처리가 가능하다.

마지막으로 의료서비스와 의료보험 급여에 대한 이의제기를 해결하는 절차의 질과 비용효과성을 확보하기 위한 경우처럼, 사회 보호 영역에서 공공이익을 위한 경우에 개인 건강정보의 처리가 가능하다. 다만 정보주체의 동의 또는 유럽 연합이나 회원국의 법에 특별한 규정이 없다면 이 개인 건강정보가 다른 목적을 위해 사용되어서는 안 된다.

이와 달리 역사, 통계, 과학적 연구를 위하여 개인 건강정보를 사용하는 것은 당사자의 동의와 규칙안 제83조에 규정된 요건과 보호조치 하에서만 허용된다. 다만, 회원국은 공익성이 높은 연구의 경우 다른 방법으로는 진행될 수 없다면 연구에 대한 동의요건에 대한 예외를 규정할 수 있다. 이 경우 개인정보는 익명화해야 하며, 만일 익명화하는 경우 연구

의 목적을 달성할 수 없다면 고도의 기술적 기준에 따라 가익명화를 하고 필요한 모든 수단을 사용하여 권한 없이 재식별화하는 것을 예방해야 한다.

3) 정보보호기본규칙안의 의미

개인 건강정보는 가장 내밀한 개인정보의 하나로서 강력한 보호가 필요하다. 그러나 이러한 정보의 사용을 위해서 예외 없이 정보주체의 동의를 요구한다면 공중보건상의 위협에 합리적으로 대처하는 것은 매우 어렵다.

1995년 EU의 개인정보보호지침은 예방의학, 의료서비스 관리 목적으로 직업적 비밀유지 의무가 있는 보건의료 전문가가 자료를 처리하는 경우 정보주체의 명시적 동의가 없이도 진료정보를 사용할 수 있다는 예외적 조항을 규정하고 있었지만 일부 국가만이 이를 허용해 왔다.

이런 상황에서 2014년 EU의 정보보호기본규칙안은 더욱 명료하게 공중보건을 위한 개인정보의 사용에 대하여 언급하고 있는 것이다. 특히 이 정보보호기본규칙안은 공중보건을 위하여 개인정보를 처리하는 것을 역사, 통계, 과학적 연구를 위하여 개인정보를 처리하는 것과 분명하게 구별하고 있다. 특히 전자의 경우 일정한 요건 아래 정보주체의 동의 없이 개인정보를 사용하는 것을 허용하고 있다. 그리고 역사, 통계, 과학적 연구일지라도 공익성이 높은 연구의 경우 회원국은 익명화 혹은 가익명화 등의 요건에 따라 정보주체의 동의에 대한 예외를 규정할 수 있다고 규정하고 있다. 이러한 EU의 정보보호기본규칙안은 공익과 사익의 합리적 균형을 유지하기 위해 노력하고 있다고 평가할 수 있다.

결론

여러 요인 때문에 우리나라에서 보건의료 부문의 전산화는 상당한 정도로 진척되어 있다. 전 국민 건강보험 체계 속에서 전산적 형태로 모이는 보건의료 자료의 양은 실로 방대하다. 최근 건강보험심사평가원은 보유하고 있는 환자진료, 의약품정보, 병원정보, 의약품사용평가 정보 등 연간 200억 (49.5 TB) 개에 달하는 빅데이터를 공개하기로 하고 의료정보지원센터까지 개소하였다. 그동안 건강보험심사평가원이

소극적으로 진행하던 정보공개 관행에서 벗어나 여러 가지 활용방안을 모색하는 것으로서 바람직한 모습이다. 이에 따라 관련 연구자들은 건강보험심사평가원의 자료와 국민건강영양조사 자료와의 연계를 통한 활용방안까지 내놓고 있다.

그러나 건강정보의 보호와 활용이라는 얼핏 상충되어 보이는 정책목표에 대하여 근본적인 검토 없이 시류에 편승하여 관련 업무를 진행해 나간다면 곧 벽에 부딪칠 것이다. 심각한 정보유출 사건이 발생하고 다수의 피해가 발생하면 다시 빅데이터에서 빅브라더로 여론이 뒤바뀔 수 있기 때문이다. 합당한 보호대책을 고민하지 않고 광범위한 개인정보 활용이 허용된다면 개인의 자유는 극도로 축소될 수도 있다. 따라서 건강보험심사평가원의 자료와 국민건강영양조사 자료와의 연계를 통한 활용방안 등 공익 목적을 위한 건강정보의 활용에 대하여 깊이 있는 논의와 충분한 사회적 합의가 선행되어야 한다.

문제는 최근 개정되어 전면 시행되고 있는 개인정보보호법은 공중보전과 같은 공익 목적을 위한 개인 건강정보의 사용에 대하여는 아무런 고려가 없다는 점이다. 제정 과정에서 이와 관한 논의나 의견수렴은 거의 없었다. 반면 개인정보를 엄격하게 보호하는 1995년 EU DPD조차 직업적 비밀 유지 의무가 있는 보건의료 전문가가 공익 목적으로 자료를 처리하는 경우 정보주체의 명시적 동의가 없이도 진료정보를 사용할 수 있는 길을 열어두고 있다.

더 나아가 최근 EU 의회를 통과한 정보보호기본규칙안은 공중보전 전문가들의 의견을 반영하여 일반적인 학술 연구와 구분하여 공중보전을 위하여 개인정보를 사용하는 것을 분명하게 허용하고 있다. 이러한 내용은 서구 사회에서 정보주체의 동의가 없다면 개인정보의 사용을 절대 허용하지 않는 것처럼 생각하는 통상적인 이해와는 크게 다른 것이다.

우리나라에는 이미 정부의 행정목적들을 위하여 정보주체의 구체적 동의 없이 각종 자료를 연계하도록 허용하는 법령이 존재한다. 대표적인 예가 사회복지통합전산망과 관련된 법령이다. 사회복지사업법은 복지 요구의 조사와 관련하여 보건복지부장관이나 지방자치단체의 장이 금융·국세·지방세·토지·건물·건강보험·국민연금·고용보험·산재보험·출입국·병무·보훈급여·교정(矯正)·가족관계증

명 등 대통령령으로 정하는 관련 전산망 또는 자료를 이용하여 경우에는 관계 기관의 장에게 협조를 요청할 수 있다고 규정하고 있다[15].

이러한 입법례는 개인정보의 관리에 있어서도 공익과 사익의 조화가 필요하다는 점을 알려준다. 그러나 아무리 공익적 목적을 위하여 정보추체의 동의 없이 개인정보의 처리를 허용한다 하더라도 개인정보보호 대책을 명확하게 규정하지 않고 있다는 점은 개선해야 할 것이다. 유럽의 관련 전문가들은 공중보전을 위한 개인정보의 처리가 필요하다는 점을 역설하면서도 이를 위해서는 “자료설계부터 프라이버시를 보호(privacy by design)”해야 한다는 개념을 정보보호 기본규칙안에 담아내고 있다. 우리나라에서도 엄격한 개인정보보호 조치를 마련함과 동시에 공중보전을 위하여 개인정보처리를 가능하게 하는 입법적 조치가 필요한 시점이다.

찾아보기말: 개인 건강정보; 사생활; 동의; 공공이익

ORCID

Hyoung Wook Park, <http://orcid.org/0000-0002-7049-7812>

REFERENCES

1. Constitution of the Republic of Korea. Article 17 (Oct 29, 1987).
2. Kwon GB. The protection of personal information and self-information control right. Seoul: Kyungin Publishing; 2005.
3. Carinci F, Di Iorio CT, Ricciardi W, Klazinga N, Verschuuren M. The position of the European Public Health Experts Workshop on privacy protection on the revision of the EU data protection directive [Internet]. Brussels: European Commission; 2011 [cited 2014 Apr 21]. Available from: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/euphex_en.pdf.
4. Kim SG. The policy issues of Personal Information Protection Act. In: Korean Association for Policy Studies. 2011 Spring symposium proceedings; 2011 Apr 15; Seongnam, Korea. Seoul: Korean Association for Policy Studies; 2011. p. 559-579.
5. Personal Information Protection Act. Law No. 11690, Article 2-1 (Mar 23, 2013).
6. Personal Information Protection Act. Law No. 11690, Article 18-2 (Mar 23, 2013).
7. Enforcement Rule of the Personal Information Act, Ordinance of the Ministry of Health and Welfare No. 213. Articles 9, 12, 14, 15 (Oct 4, 2013).

8. Ministry of Security and Public Administration. Application of Personal Information Protection Act to medical institution [Internet]. Seoul: Ministry of Security and Public Administration; 2012 [cited 2014 Apr 21]. Available from: http://www.mospa.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=29268.
9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Internet]. [place unknown]: EUR-Lex; 1995 [cited 2014 Apr 21]. Available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.
10. European Commission. A comprehensive approach on personal data protection in the European Union [Internet]. Brussels: European Commission; 2010 [cited 2014 Apr 21]. Available from: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
11. European Union. European Commission sets out strategy to strengthen EU data protection rules [Internet]. Brussels: European Union; 2010 [cited 2014 Apr 21]. Available from: http://europa.eu/rapid/press-release_IP-10-1462_en.htm.
12. European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data [Internet]. Brussels: European Commission; 2012 [cited 2014 Apr 21]. Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
13. European Commission. Progress on EU data protection reform now irreversible following European Parliament vote [Internet]. Brussels: European Commission; 2014 [cited 2014 Apr 21]. Available at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.
14. European Parliament. Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): compromise amendments on Articles 1-29 [Internet]. London: European Parliament; 2013 [cited 2014 Apr 21]. Available from: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf.
15. Social Welfare Services Act. Law No. 11239, Article 33-3 (Jan 26, 2012).

Peer Reviewers' Commentary

본 논문은 보건의료 분야에서 현재 이슈가 되고 있는 디지털 정보에 대한 활용의 법과 정책에 관한 EU의 입법 상황을 다룬 글이다. 빅데이터 활용과 개인 프라이버시권의 충돌을 해결하기 위한 EU의 법과 정책은 흔히 미국의 연방 입법에 비하여 개인의 권리 보호에 좀 더 충실하다는 평가를 받고 있다. EU의 개인정보보호에 관한 1995년 지침(Directive), 전자개인정보에 관한 2002년 지침, 1995년 지침에 의한 정보위원회에서 제정한 2007년 전자보건의료(Electronic Health Records)보고서가 기존에 논의되었던 주요 내용이고, 본 논문은 1995년 지침에 관한 개정 논의로서 2010년 논의, 2010년 논의에 대한 보완으로서 공중보건의료를 추가한 2014년 지침 개정을 설명하고 있다. EU의 최신 입법과 정책을 체계적으로 기술하고 있는데, 한국의 논의 발전을 위한 방향 제시를 했다는 점에서 의미가 있는 논문이라 판단된다.

[정리: 편집위원회]