의료정보 비식별화와 해결과제

우성희

한국교통대학교

De-identification of Medical Information and Issues

SungHee Woo

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr

요 약

빅데이타의 활용과 개인정보보호의 균형점을 찾기 위해 등장한 것이 비식별화이다. 특히 다양한 준식별자 정보 및 민감정보를 처리하는 의료분야에서는 EMR 및 음성, 카카오톡과 같은 의료 상담, SNS 등의 자료 사용을 위해서는 반드시 비식별화를 하여야 한다. 하지만 이를 위한 독립된 의료정보 보호법 및 비식별화를 위한 법제화도 되어 있지 않는 상황이다. 따라서 본 연구에서 국내외 개인정보 비식별화 현황, 의료정보 비식별화 현황 및 사례 그리고 의료정보 보호와 비식별화를 위한 해결과제와 이슈를 제시한다.

ABSTRACT

It is de-identification that emerged to find the trade-off between the use of big data and the protection of personal information. In particular, in the field of medical that deals with various semi-identifier information and sensitive information, de-identification must be performed in order to use medical consultation such as EMR and voice, KakaoTalk, and SNS. However, there is no separate law for medical information protection and legislation for de-identification. Therefore, in this study, we present the current status of de-identification of personal information, the status and case of de-identification of medical information, and finally we provide issues and solutions for medial information protection and de-identification.

키워드

의료정보 비식별화, 의료정보보호, 빅데이터

Ⅰ. 서 론

빅데이타와 함께 등장하는 것이 개인정보보호이며 이 두 가지의 균형점을 유지하기 위해 나온 것이 비식별화이다. 최근 비식별화는 빅데이타 활성화를 위한 빅 이슈가 되고 있다. 따라서 국내외적으로 비식별화 조치 가이드라인[1]이 제시되고 있지만 특히 의료정보에 대한 가이드라인은 미흡한 상황이다. 미국과 프랑스는 환자의 개인정보 및 의료정보가 수록되어 있는 기록의 발생부터 관리 및 법을 이행하지 못했을 경우의 처벌 조항까지 체계적으로 규정하고 있으며 기록의 작성자인 의사와 의료기록의 주체인 환자간의 기밀유지와 사생활 보호에 대해 중점적으로 법으로 규정하고 있다. 현재 우리나의 경우 의료기관의 특수성으로 인해 개인정보보호법과 의료법은 준용하여 사용하고 있으나 서로 매칭되지 않는 부분들과 애매한 법조항으로 인해 혼란을 겪고 있다. 이미 국내에서는 개인 의료정보 유출 피해 사건들이 발생하여 의료정보의 민감사항을 침해했을 경우에 대한 보다 체계적이고 구체적인 의료정보보호법이 필요하다. 따라서 본 연구에서는 국내외 개인정보 비식별화 현황, 의료정보 비식별화 현황 및 사례 그리고 의료정보보호와 비식별화를 위한 해결과제와 이슈를 제시한다.

Ⅱ. 개인정보 비식별화 현황

개인정보보호 관련 정부부처 등의 기관이 모여 정부차원의 모든 분야에 적용 가능한 비식별화 조치 가이드라인[1][2]이 2016년 6월 30일 발표되었다. 이는 개인정보를 비식별 조치하여 이용 또는 제공하려는 사업자 등이 준수 하여야 할 조치 기준을 제시한 것으로 정보주체를 알아볼 수 없도록 비식별 조치한 후 비식별 정보는 개인정보가 아니므로 빅데이터 분석 등에 활용이 가능하다는 것이다. 이것은 개인정보보호법의 개인정보의 정의를 해석해 개인정보 처리자에 의한 입수 가능성을 고려한 것으로 개인정보보호법 제18조 2항 4호에 근거하고 있다. 또한 개인정보 침해위험을 최소화할 수 있는 방안으로 개인정보 비식별화 조치는 매우 중요한 수단이 될 수 있다. 해외 비식별화 조치 가이드라인을 보면 다음과 같다[3][4].

표 1. 해외 비식별화 가이드 라인

	명칭/용어	발행기관	발행시기	비식별화처리원칙
영국	익명화 : 데이터보호 위험관리지침/익명화	영국 독립 정보 감독청	2012년 11월	정보주체를 식별할 수 없도록 익명화
호주	데이터 및 개인정보의 비식별화/비식별화	호주 독립 정보 감독청	2014년 4월	개인식별정보 삭제, 독특한 정보와 결합이나 특징으로 개인이 식별될 수 있는 정보 삭제 또는 변경
미국	개인정보 비식별화/비식별화	미국 국립 표준 기술원	2015년 10월	정보주체와 데이터셋 연관성 제거
유럽	일반정보보호규정(GDPR)/가명화	유럽연합(EU)	2015년 12월	특정 개인에게 연결 삭제
일본	익명가공정보,개인정보보호법/익명가공정보	개인정보보호법	2015년	익명가공정보등 새로운 유형의 개인정보 개념 도입

미국의 경우 데이터 비식별화는 수집된 데이터에서 개인정보를 제거하기 위한 수단이며 하나의 기법이 아니라 여러 다른 방법, 툴, 알고리즘의 집합으로 수행되는 프로세스, 특정정보 주체와 식별 데이터 집합간의 연계를 제거하기 위한 프로세스로 지칭하고 있으며 비식별화 데이터 처리 모델을 제시하고, 계약에 의해 이용되거나 제 삼자에게 공개될 수 있도록 했다. 영국은 익명화는 데이터를 정보주체를 식별할 수없는 형태로 만들거나 식별이 발생하지 않도록 하는 과정으로 정의되고 있다. 또한 데이터 마스킹, 가명화, 총계처리 등의 익명화 기법이 소개되고 있으며 재식별화(re-identification) 위험이 없도록 효과적인 익명화를 보장할것을 요구하고 있다. 호주의 비식별화는 개인 식별자(이름, 주소 등)를 제거하고 개인을 식별할 가능성이 있는 다른 정보(개인특정이 가능한 드문 속성 정보)를 제거하거나 변경하는 두 단계로 구성된다. 유럽연합의 경우 가명화 할 때는 실명화 되지 않기 위한 기술적 조치를 요구하고 있다. 암호화 등을 통해 이 요구에 부응할 수 있으며, 암호화 등으로 데이터를 인식불가능하게 한 경우에는 데이터유출시 정보주체에게 통지하는 의무를 면제받도록 하였다. 제83조에서는 과학, 역사, 통계 목표의 이용을 위해 가명화한 후 정보를 이용할 수 있도록 허용하고 있다. 일본은 빅데이터를 기반으로 다양한 신규 비즈니스 기회를 창출하고 경제재생계획을 실현하기 위해 기존 빅데이터 관련 규칙을 강화한 것이 특징이며 개정된 개인정보보호법은 익명가공정보등 새로운 유형의 개인정보 개념 도입, 옵트 아웃방식의 개인정보 이용목적변경에 관한 규정 전환, 개인정보의 이용 및 활용에 관한 민간기구의 설립, 개인정보개시청구권 인정 등을 주 내용으로 하고 있다.

III. 의료정보 비식별화 현황 및 사례

환자의 의무기록을 포함한 건강에 관한 정보는 개인정보 보호법상 민감정보[6]로 분류되어 개인정보 보호 이슈가 되고 있다. 국내외 의료정보 비식별화 사례를 보면 다음과 같다.

1) 국내

국내 의료정보 비식별화 사례[7]로 국민건강 주의 예보 서비스, 보건의료 빅데이터 활용 서비스, 빅데이터 기반 의약품 안전성 조기경보 서비스의 내용과 분석기법, 비식별화 방법, 처리기법등을 살펴보면 다음 표 2와 같다. 국민건강 주의 예보 서비스의 경우는 주요 감염병 유행을 예측하여 관련 기관과 국민 개개인이 유행에 대비하고 예방할 수 있도록 지원함으로써 국민건강 증진 및 사회적 편익 극대화를 시킬 수 있고, 보건의료 빅데이터 활용 서비스는 공중보건 분야의 전염병 발생 및 불법 약물 전파와 같은 긴박한 순간에 미리 대비하고, 빠른 의사결정을 도움으로써 의료대응와 관련한 사회적 비용 대폭 절감할 수 있다. 그리고 빅데이터 기반 의약품 안전성 조기경보 서비스는 빅데이터를 활용, 국민복지와 건강을 위협하는 의약품 부작용 및 오남용을 조기에 발견하여, 선제적 대응을 통한 안전한 사회 구현에 기여할 수 있다.

표 2. 의료정보 비식별화 국내사례

	국민건강 주의 예보 서비스	보건의료 빅데이터 활용 서비스	빅데이터 기반 의약품 안전성 조기경보 서비스
주요 내용	유행성 질병관련 종합정보 제공 및 건강보험 정보와 소셜미디어 정보 융합, 질병 예측 모델 개발	보건의료 질 향상 및 비용 절감을 위한 보건의료 빅데이터 활용 서비스 개발	의약품 부작용 및 오남용 사례를 수집 및 분석, 의약품 부작용 가능성 조기 인지, 약품 오남용 사례 파악하여 조기 대응정보 제공
활용 데이터	국민건강보험공단(국민건강정보), 다음소프트(SNS 데이터)	검색 및 SNS 데이터, 입/퇴원 기록, 병원 경영자료, 실시간 환자 심전도/심박수, 진료 데이터, 국과수 마약류 관련 DB, SNS 데이터	와이즈넛(SNS), 뉴스(웹), 문헌(웹) 데이터, 아주대학교병원(EMR)
비식별화 대상	개인정보(주민등록번호, 연령, 주소, 요양기관기호), 사생활정보(소득, 민감상병)	성명, 전화번호 등의 일체 개인정보, 건강보험증번호, 바이오정보, 홈페이지 회원 ID, 사번, 비밀번호	개인정보, 사생활정보(아이디, 진단명, 약처방 날짜, 진단검사 날짜, 검사수행 날짜)
비식별화 처리법	가명처리, 삭제, 마스킹, 범주화	가명처리, 삭제, 마스킹	가명처리, 삭제, 범주화

2) 국외

개인정보 활용이 가장 활발하게 이뤄지는 영역 중 하나가 의료 분야인 만큼 국외의 의료 개인정보 비식별화 적용 및 식별가능 정보 이용에 대한 법제, 관련 기관들의 움직임과 주요 사례, 향후 과제 등이 더 정교화 되거나 활발하게 논의되고 있다. 미국과 영국의 현황과 사례[3][4]를 보면 다음 표 3과 같다.

표 3. 의료정보 비식별화 해외사례

	미국	영국
비식별화 방식	HIPAA에 연계된 HIPAA 프라이버시 규칙 제시	국민보건서비스인 NHS의 익명화 표준 제정
사례	ONC: 전자화된 보건의료정보를 이용하여 의료 서비스 공급자와 소비자, 보건의료 행정가 및 정책입안자 등 다양한 이해관계자의 의사결정 지원	보건복지정보센터(Health and Social Clinical Information Center, HSCIC) : 재구성한 데이터를 수요자의 요구에 따라, 환자 수준의 식별 가능한 정보, 익명화 또는 가명화한 비식별화 된 정보 제공

미국의 경우 의료정보의 비식별화 방식은 HIPAA에 연계된 HIPAA 프라이버시 규칙을 통해 제시된다. HIPAA 프라이버시 규칙에서는 제한적인 데이터세트(Limited Data Set, LDS)도 규정하고 있다. 제한적인 요건 하에서 정보주체의 동의나 허가 없이도 데이터를 이용하거나 제공할 수 있는 LDS는 18개 식별자중 직접적 식별자에 해당하는 16가지 식별자를 제거하거나 데이터를 제공받는 자와 데이터이용 계약를 체결하면 인정받을 수 있다. ONC(The Office of the National Coordinator for Health Information Technology)는 전자화된 보건의료정보를 이용해 의료 서비스 공급자와 소비자, 보건의료 행정가 및 정책입안자 등 다양한 이해 관계자의 의사결정을 지원한다.

영국은 의료 관련 데이터는 정보보호법과 보건부의 지침 등에 따라 엄격한 기준과 심사를 거쳐 제한적으로 활용된다. 전자의무기록의 활용을 위한 가이드라인도 정비되어 있다. 영국의 국민보건서비스인 NHS는 의료분야에서 정보보호와 정보공개라는 두 가지 목적을 충족시키기 위해 2013년 2월 건강 및 소셜 케어 데이터의 공표를 위한 익명화 표준을 제정하였다. 보건의료서비스 전달체계에서 혁신과 가치향상을 위해 의료 정보의 보고와 분석 등 다양한 용도로 사용할 수 있도록 구축한 SUS(Secondary Uses Service)는 의사의 진료를 제외한 다른 목적으로 사용할 수 있는 환자 정보를 보건의료계획, 지불제도, 서비스 전달체계 개선, 공중보건사업 등의 의료 관련 정책 사업을 위해 사용할 수 있도록 하고 있다. 이외에 프랑스는 의료정보보호를 위한 공공보건법을 시행하였고, 캐나다는 독립된 의료정보보호법이 실행되고 있다.

Ⅳ. 해결과제와 이슈

개인정보보호와 동시에 효율적인 의료정보 빅데이타 활용을 위해 선행되어야 과제와 이슈는 다음과 같다.

1) 의료정보의 명확한 정의와 일반 의료정보와 실 사용항목 구분, 주체 간 합의

개인정보에 대한 비식별화 규정들은 HIPAA 프라이버시 규칙 내용을 기반으로 하고 있어 사실상 의료부문, 의료정보에 범용적으로 적용한다. 그러나 국내 의료관련 법령인 의료법, 국민건강보험법, 의료 급여법, 감염병 예방 및 관리에 관한 법률, 응급의료에 관한 법률등 그 외 관련 다수 법등에서 규정하고 있는 의료정보는 진단서, 의료급여증, 건강보험증, 예방접종증명서, 응급환자 진료의뢰서등 관련 다양한 서식에 인적정보, 질병정보뿐 아니라 기관정보, 행정정보 등 다양한 정보가 포함되어 있다. 개인의 질병치료, 관리 및 예방을 위한 정보들을 의료정보라는 하나의 용어로 표현

하고 있다. 따라서 개인의료정보 비식별화 조치범위 등의 명확화가 어려워 현장에서는 세부영역에 따라, 적용하는 관계자에 따라 달라질 수 있다. 또한 개인의료정보란 의료정보 전체가 아닌 개인식별성을 가지는 정보에 한정되어야 하므로 의료정보 및 의료정보 종류에 대해 보다 명확한 정의가 되어야 한다. 일반 의료정보와 개인의료정보 중에서도 해당정보 자체로 식별성을 지닌 정보와 타 정보와 쉽게 결합하여 식별 가능한 정보에 대한 실 사용항목을 예로 한 구분이 필요하며 이에 대해 다양한 주체간 합의 또한 선행되어야할 것이다[5].

2) 독립된 의료정보보호법 제정

보건의료정보 인프라 구축이 일반화되어 편의성과 신속성은 증대되었지만 개인정보 유출 및 노출의 위험성은 더 커지고 있다. 국내에서는 일반법으로서 개인정보 보호법과 정보통신망법을 제정·시행하고 있고, 여기에 의료법, 국민건강보험법, 생명윤리 및 안전에 관한 법률 등에서 인간대상 연구에 참여하는 개인의 정보보호를 규정하고 있고 최근에 개인정보 침해위험을 최소화할 수 있는 방안으로 개인정보 비식별화조치에 대한 가이드라인, 지침, 사례집 등이 발표되었다. 하지만 의료정보에 대한 가이드라인은 부재하다. 따라서 개인의 병력과 가족력, 유전정보, 그리고 기타 사적인 정보를 모두 포함하는 개인의료정보의 보호와 의료정보의 명확한 개념 정의, 대상과 범위, 관계자 책임의 의무, 관리 이용 절차와 방법에 대한 법규가 제정되어야 할 것이다[5][8].

3) 비식별화를 위한 법제화

개인정보 보호와 활용은 서로 다른 양면성을 가지고 있다. 따라서 이를 위한 타협안으로 가이드라인에 근거한 비식별화를 위한 법제화가 필요하고 비식별화 전문기관 요건과 비식별화 데이터의 정의, 비식별화 데이터 안전성 등의 법적 근거 공고화를 위한 법제화 노력 또한 요구된다. 이와 더불어 비식별화 관련 기술과 프로세스에 대한 국제 표준화에 참여 및 글로벌 비즈니스 환경을 고려하여 국제 표준에 근거한 체계, 기술과 프로세스의 적용이 요구된다[8].

Ⅴ. 결 론

빅데이터란 용어는 지금 매우 익숙한 단어가 되었다. 빅데이터 활용 시장의 가치와 시장규모는 점점 커지고 있지만 이러한 데이터 활용에 있어 개인정보보호는 가장 큰 이슈로 떠오르고 있다. 데이터의 활용과 개인정보 보호는 같이 동반 되어야 한다. 따라서 데이터 활용과 개인정보보호를 동시에 고려하면서 등장한 것이 바로 비식별화이다. 특히 다양한 준식별자 정보 및 민감정보를 처리하는 의료분야에서는 EMR 및 음성, 카카오톡과 같은 의료 상담, SNS 등의 자료 사용을 위해서는 반드시 비식별화가 되어야 한다. 하지만 비식별화에 대한 명확한 기준을 제시하고 있지 않다. 또한 비정형 데이터는 암호화만 언급될 뿐 활용에 대해서는 논의되지 않고 있다. 따라서 의료정보가 활용 가능한 의미 있는 비식별화 데이터가 되기 위해서는 정보운영 형태를 체계적으로 통합하고 위탁병원 및 체인병원간의 데이터연계 방안 수립 등을 통해 뒷받침할 수 있는 기준을 마련해야 할 것이다.

참고문헌

[1] “개인정보 비식별 조치 가이드라인”, 미래창조과학부 보건복지부, 2016. 6.
[2] “개인정보 비식별화기술 활용 안내서”, 미래창조부, NIA, 2015. 6.
[3] “개인정보 비식별화 관련 해외 현황 및 사례” 한국인터넷 진흥원, 개인정보보호 핫이슈 심층 분석 보고서, 2016.5.
[4] 염홍열, “빅데이터 관련 개인정보 비식별화 정부 가이드라인 수립”, KISO JOURNAL vol.24.
[5] 정영철, “의료분야 빅데이터 활용을 위한 개인정보 비식별화 규정 현황과 과제”, 보건복지포럼, 2015.9.
[6] 신수용, “개인정보보호를 위한 헬스케어 데이터 익명화”, 한국정보과학회지, 2017.2.
[7] “빅데이타 활용을 위한 개인정보 비식별화 조치 사례집”, 미래창조과학부 2014.5.
[8] 박민영, 최민경, “의료정보의 관리와 비식별화에 대한 법적 과제”, 유럽헌법연구 vol.21, 2016.8.